Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

Steering Government into the Next Millennium:

A Guide to Effective Business Continuity in Support of the Year 2000 Challenge

October 14, 1998
Enhanced Management Framework for IT
Chief Information Officer Branch
Treasury Board of Canada Secretariat

Canada

PUBLICATION HISTORY

Version	Release Date	Revisions
0.1	June 1, 1998	Table of Contents only. For discussion purposes only.
0.2	June 11, 1998	First Draft for Kate Dobson's review only. Quality assurance was not done on this document.
0.3	June 15, 1998	Second Draft for TBS review only.
0.4	June 17, 1998	Final Version for Distribution to Translator
0.5	June 17, 1998	Final Version for Editing
0.6	June 17, 1998	Edited Version
0.7	June 18, 1998	Draft for final review
1.0	June 18, 1998	Final Draft
1.1	June 26, 1998	Final
2.0	September 25, 1998	Version 2.0
2.1	September 28, 1998	Version 2.1 for final review
2.2	October 14, 1998	Version 2.2 Final

TABLE OF CONTENTS

LIST OF APPENDICES

Preface

Background

The Canadian federal government, like most public and private sector organizations will be facing a problem when the year changes from 1999 to 2000.[1] Many systems that use a date in their processing, have traditionally utilized the date as a two-digit reference instead of a four-digit reference. The change to a new millennium may result in an error in date-related processing unless changes are made to these systems.

The potential negative consequences of the Year 2000 problem are far reaching and could bring entire organizations to a halt, or at least significantly impact their ability to deliver their services or products. Within the context of the federal government, the consequences could have highly undesirable impacts on Canadians, the country, and its economy. Specifically, these problems relate to inaccurate date processing or “denial of government service” issues when the systems crash.

The Treasury Board of Canada Secretariat (TBS) has initiated a project to address the Year 2000 problem across the government. A Project Office was established to initiate activity and to facilitate and monitor the progress on converting assets supporting government-wide mission-critical functions. A preliminary assessment of the significance of the Year 2000 problem across the government determined that 48 government-wide mission-critical functions might be sensitive to this problem.

The latest readiness assessment[2] of the government’s progress in solving the Year 2000 problem shows that there is still a significant amount of work to be completed before the year 2000. The current project status suggests that government departments must consider the possibility that government services and programs will be affected by Year 2000 failures. Within that context, TBS is taking a leadership role in advising departments to:

a) Assess what could go wrong;
b) Develop contingency plans as required;
c) Ensure that departments have in place the proper framework to manage crises related to Year 2000 and associated events; and
d) Plan for full business resumption, following a Year 2000 related business interruption.

Specifically, TBS is providing departments with this guide to business continuity, which will enhance the government’s ability to address the potential negative consequences of the Year 2000 problem.

[1] There is also a related issue about leap year processing from the “extra” leap year for Feb 29, 2000.

[2] Braiter/Westcott Report on Year 2000 Readiness, February 1998.

Why this Guide was Developed

This guide was developed to:

a) Help departments manage risks associated with their Year 2000 initiatives, and ensure uninterrupted and fully functional delivery of programs and services to Canadians in spite of Year 2000 related failures;
b) Help departments identify business continuity issues and properly prepare to manage Year 2000 problem related crises; and
c) Help the TBS ensure that departments are ready to face the potential negative consequences of the Year 2000 problem and that the government is aware of the risks and consequences associated with not solving the Year 2000 problem.

Purpose of this Guide

The purpose of this document is to present a uniform and standardized set of business continuity activities for all departments to implement in order to facilitate the government's governance of the Year 2000 problem and thereby increase its likelihood of success.

Acknowledgment

TBS would like to acknowledge the contributions of the following participants:

a. ***Godcharles Goulet Fournier Consulting Inc.*** for developing this guide;
b. Veterans Affairs Canada for initiating the process;
c. The Software Engineering Institute, for allowing us to use their risk management material;
d. The departments of Fisheries and Oceans Canada, Agriculture and Agri-Food Canada, Public Works and Government Services Canada and Human Resources Development Canada for sharing some of their process artifacts; and
e. Magellan Engineering Consultants Inc. for their contribution in the areas of crisis response and business resumption.

1
Introduction to the Guide

1.1 Why Focus on Business Continuity?

Like all projects of this nature, size and complexity, the Year 2000 project brings with it a significant amount of uncertainty, unexpected events resulting from the dynamic environment in which we live in, and undesirable outcomes from the remediation work performed by departments. Most people would agree, in that context, that continuous risk management would be beneficial to departments. Who wouldn't want to identify potential problems early enough so that they can be addressed, thereby helping to ensure the ultimate success of their Year 2000 initiatives?

The Government remains optimistic about the its ability to successfully address the Year 2000 problem, but it is the ethical, social, business, and legal responsibility of all government managers to consider the possibility of not being able to complete their conversion activities. Continuity of operations should be the prime concern of managers impacted by the Year 2000 problem. Contingency planning will put these managers in a position to pro-actively and positively work through a potential crisis due to a Year 2000-related business disruption. A pre-established framework for control as well as effective communication, practiced through realistic scenarios, will also provide managers with invaluable tools to work through potential crises.

For these reasons, it is critical that business continuity be a priority for all departments.

1.2 Business Continuity Concepts and Definitions

In order to clearly position the business continuity process described in this guide vis-à-vis similar processes at the government and national level and conversion activities taking place within the departments, we are providing the readers with the underlying concepts of our process and some basic definitions. At the conceptual level, the TBS business continuity process can be depicted as shown below in Figure 1.

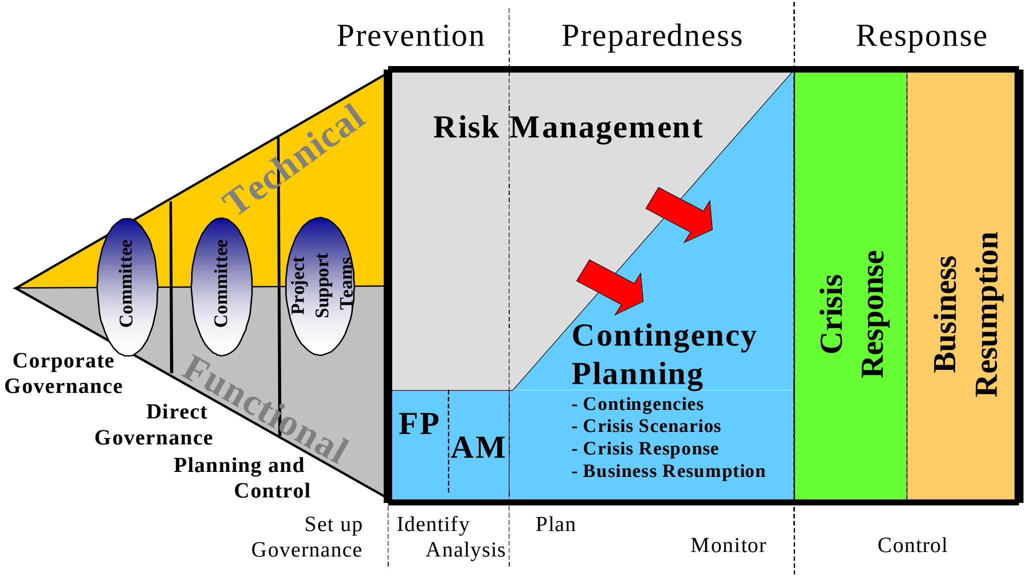


Figure 1 – Conceptual View of the Business Continuity Process

The Business Continuity process start with the establishment of a governance structure which will steer the process and ensure that decisions are made in a timely fashion. The governance structure extends from the planning and control level, where resources are mobilized and assigned to conversion activities, to the corporate (or department level) governance where high level decisions are made regarding business continuity. Both sides of the organization, that is functional and technical, are represented and bring their own set of objectives to the process. Technical personnel aim at achieving Year 2000 compliance before the year 2000 while functional personnel aim at ensuring business continuity. This guide is targeted at the functional side of the organization but recognizes that the achievement of the functional personnel's objectives is heavily dependent on the technical personnel's ability to meet theirs. The technical side of the organization plays an important role in the performance and success of the business continuity process.

The business continuity process spans over the three stages of business continuity identified, within the context of this guide, as:

a. **Prevention**. This is the period where organizations identify risks that may impact the continuity of their business processes, evaluate the key attributes of the risks, and determine the organization's response to these risks in order to reduce their exposure to business interruptions;

b. **Preparedness**. The preparedness stage aims at establishing the plans to address the risks and monitor the progress of the conversion work and evolving the business continuity plan; and

c. **Response**. The final stage follows the declaration of a crisis and includes working through the crisis and resuming the operations of the organization.

The Business Continuity process is then broken down into process areas which include:

d. **Risk Management**. Risk Management is a continuous process with methods and tools for identifying, analyzing, planning, monitoring and controlling potential, undesirable events which may negatively impact an organization's objectives. It should be noted that while the aim of the business continuity process is to prevent or minimize business interruptions due to the Year 2000 related failures, technical risks must also be managed since they will often constitute the root cause for these business interruptions. Risk management provides a disciplined environment for pro-active decision-making that:

   - Continuously assesses what could go wrong;
   - Determines which risks are important to deal with; and
   - Implements strategies to deal with those risks.

e. **Contingency Planning**. Contingency planning is the area of the business continuity process where a department attempts to ascertain the kinds of crises most likely to occur and prepares to deal with them. Typically based on risks deemed unacceptable or which require significant mitigation measures, the overall purpose of contingency planning is to recognize and address as many uncertainties and risks as possible so that departments can maintain control over their operations when a crisis strikes. Contingency planning includes such components as crisis scenarios, contingency plans, crisis response plans and business resumption plans;

f. **Crisis Response**. Crisis response is the collection of activities that minimize the effects of a crisis situation. Crisis response involves notification, assessment, planning, action and termination activities. Typically, this will involve the application of contingency plans to stabilize, prevent escalation and mitigate a crisis event.

Crisis response involves both direct and corporate governance as well as planning and control level personnel (Crisis Response Team) who are normally responsible for actions directed towards crisis stabilization.

g. **Business Resumption**. Typically, these are the actions undertaken once a crisis event has been stabilized. Business resumption involves the Crisis Management Team but the focus moves from the crisis itself to recovery and the resumption to normal business routines.

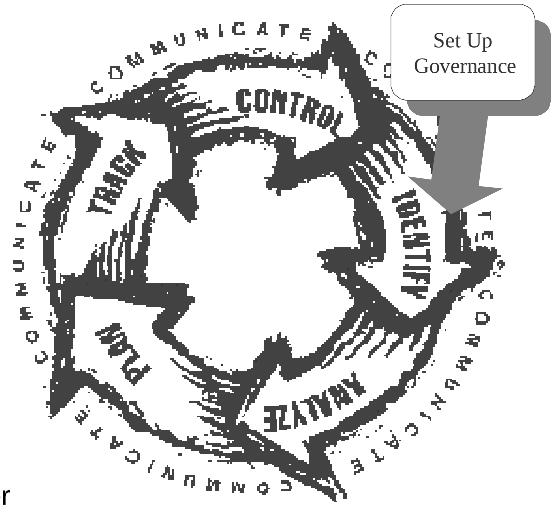
These four process areas are integrated into one common set of steps that take organizations from realizing that failures due to the year 2000 problem are possible through responding and recovering from crises. TBS integrated process has a particularity of building on the Software Engineering Institute's Continuous Risk Management process. Hence, although it may appear to differ from standard business continuity processes at the lowest level (step level), it satisfies the requirements of the government, builds upon a sound knowledge base and aligns itself nicely with similar processes implemented at the national level. These steps include:

a. Set up Governance;
b. Identify;
c. Analyze;
d. Plan;
e. Monitor; and
f. Control.

1.3 TBS Six-step Approach to Business Continuity

The TBS is proposing a six-step approach to business continuity. It builds on the work of the Software Engineering Institute for Continuous Risk Management and integrates Contingency Planning, Crisis Response and Business Resumption. The underlying activities of this approach are depicted below.

Figure 2 – Integrated Business Continuity Approach



Identify = identifier
Analyse = analyser
Plan = planifier
Track = suivre

Control = contrôler
Communicate = communiquer

The business continuity activities are as follows:

a. **Set up Governance.** The first step in implementing business continuity is to set up the required governance structure to support the process, identify and mobilize the department's resources, obtain governance structure members' commitment and involve these individuals in the business continuity process. The governance structure should not be different but integrated with the existing Year 2000 Project governance structure found in the departments;

b. **Identify.** Departments must identify risks related to the Year 2000 problem that could impact the department's ability to ensure business continuity. Departments must also identify any risks that are beyond their control and should therefore be elevated to the TBS level (government-wide issues such as public infrastructure) or shared with their partners and suppliers;

c. **Analyze.** Departments must convert the risk information, gathered in the "identify" step, into decision-making information. In addition to defining the risk attributes such as probability, impact, source and response, departments must relate the risk information to assets as well as business functions. This analysis will allow departments to clearly understand the potential impact of risk on business continuity and to take the appropriate management actions to address the risk;

d. **Plan.** Once the risks have been identified and analyzed, departments can then assign resources to the management of the identified risks, or the elaboration of contingency plans for those business functions significantly affected by risks. They should also prepare plans to respond to crises and resume business following a crisis;

e. **Track.** In order to continuously monitor risks and the related exposure to business interruptions, departments must then implement the strategies developed in the previous activity and continuously monitor variations to these plans. They must also track the progress of the conversion activities in order to identify risks; and

f. **Control.** Upon materialization of one or more risks or Year 2000 failures, departments must control the negative impacts and escalate decision requirements to the appropriate level within the governance structure. If the negative impact cannot be controlled, contingency plans or procedures may have to be implemented for the impacted business function. Under certain scenarios, a structured response to these crises will have to be initiated and special controls implemented. The control step also addresses the business resumption activities.

Implicit but critical to this approach is the need to communicate information about the possibility of not completing conversion activities and the solutions to that problem. The success of the business continuity process hinges on frank and open communications on risks, contingency plans, crisis response plans and business resumption plans within departments as well as between departments, their partners and the TBS.

1.4 Opportunities and Barriers

Getting started with this guide will probably be one of the biggest challenges for organizations that are new to business continuity. In addition to the inertia problem that many departments experience when faced with new processes, other barriers may arise. The following table summarizes some of these challenges and provides high-level solutions to address them.

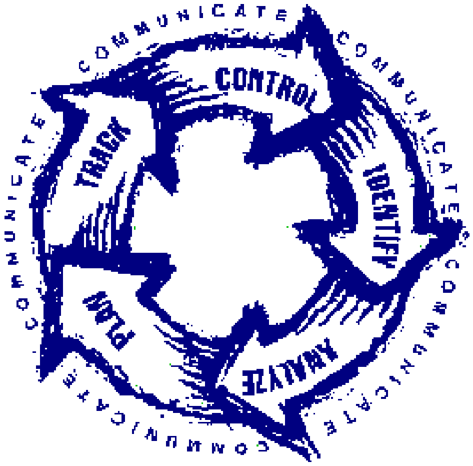
Table 1: Barriers and Solutions

Barriers	Solutions
Inadequate Senior Management Commitment	- Leverage TBS requirement for Contingency Plans by December 31, 1998 - Emphasize legal, social, ethical and business responsibilities of managers to ensure the continuity of department operations - Sell pro-active nature of the process
Insufficient Funding	- Present this process as “formalized” good management and integrate it into normal day-to-day activities - Sell the incremental nature of the process resource requirements based on progress and risk information thus minimizing the funding impact (funding gets reallocated from remediation to contingencies as failures occur or are eminent)
Cultural Barriers	- Emphasize opportunities (e.g. ability to introduce new services earlier) as well as risks - Increase the level of communication early in the process - Celebrate successes (e.g. working through unforeseen crisis, preventing problem before its occurrence, etc.)
Lack of Knowledge	- Hire temporary assistance and ensure technology transfer - Take TBS sponsored SEI courses offered through the Institute

1.5 How to Use This Guide

This guide has been structured and formatted to provide easy access to the TBS business continuity process requirements, and to maximize the efficiency of the individuals attempting to meet these requirements. The document focuses on the business continuity process and is divided into eight chapters (an introduction, six chapters describing each of the six steps, and a conclusion). The procedures required to effectively implement the elements are provided in appendices that are bound separately.

In order to keep this guide down to a reasonable size, and since the Software Engineering Institute Continuous Risk Management process has been fully endorsed by the TBS for CRM, specific references are made in this guide to the *SEI Continuous Risk Management Guidebook*. Departments that do not have a copy of the *SEI CRM Guidebook* can obtain one by contacting David Holmes at 957-2530. Activities or processes extracted directly from or based on the SEI CRM Guidebook are preceded by the logo below.



2
Set Up a Business Continuity Governance Structure

Departments must ensure that the business continuity process is supported by a sound governance structure that can steer and respond to decision requests that emerge from the process. An inadequate governance structure will impede the success and significantly impact the effectiveness of the business continuity efforts.

2.1 How to Set Up a Business Continuity Governance Structure

The first step towards implementing business continuity is to set up the required governance structure to support the process, identify and mobilize the department's resources, obtain governance structure members' commitment and involve these individuals in the business continuity process. While the business continuity governance structure should not be different but integrated within the existing Year 2000 Project governance structure found in the departments, the following generally accepted characteristics of a sound governance structure should be present during the set-up step:

a. The governance structure should extend the functional (business side) and technical (compliance side) organizations up to the point of convergence;

b. The governance structure should extend to three layers of management:
   - Corporate Governance that corresponds to the Assistant Deputy Minister levels. Deputy Ministers are normally at the point of convergence and are ultimately responsible for the performance of both sides of the governance structure;
   - Direct Governance that normally corresponds to the Director General, Director, and Year 2000 Project Manager levels; and
   - Planning and Control that corresponds to the business function owners and project leaders responsible for the day-to-day conversion activities and monitoring of the project activities;

c. Along this structure, clear accountabilities and roles should be defined regarding business continuity, including the responsibility to decide on the department's response to risks; and

d. Accountability for the continuity of operations should rest with the functional personnel; accountability for the conversion of assets should rest with the technical personnel within the organization; and committees should only be used to provide guidance and build consensus.

The governance structure is depicted in Figure 3. The remaining sections provide additional information about the tasks that must be performed in support of this activity.

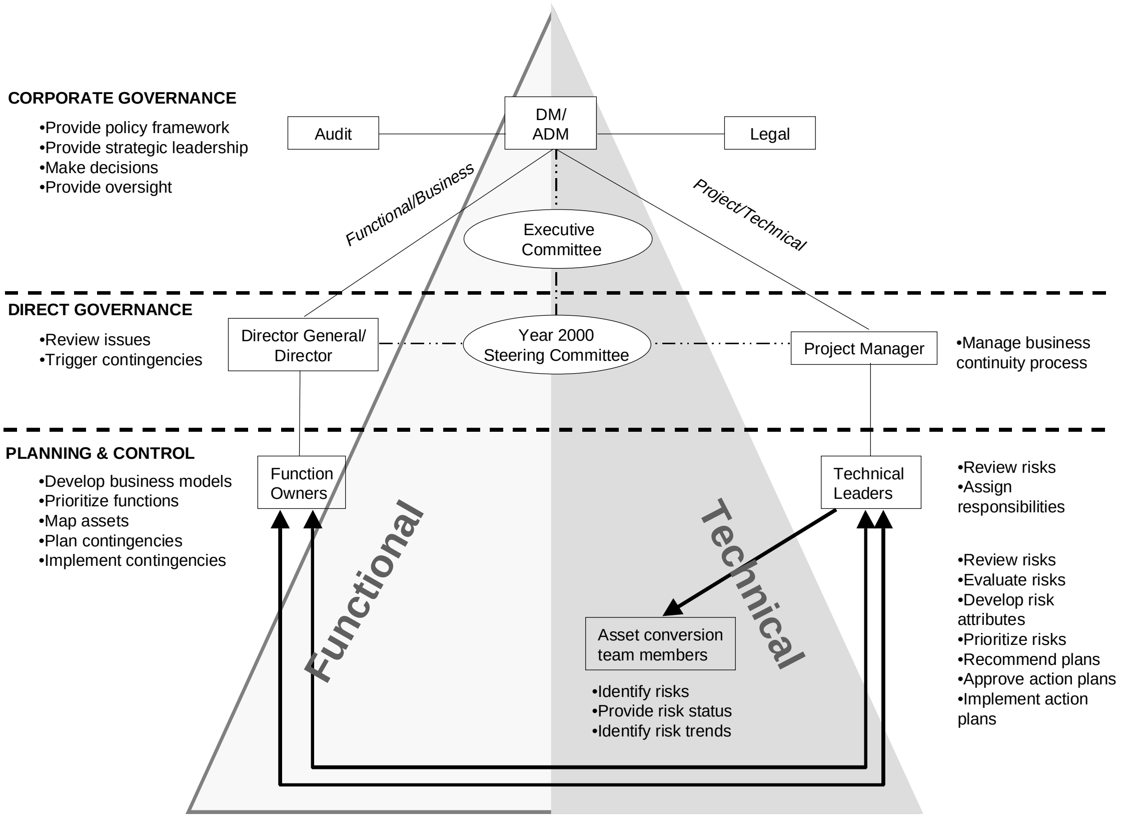


Figure 3 – Business Continuity Governance Structure

2.2 Set Up Governance

Process

The objective of this first activity is to identify the stakeholders that will be involved in the business continuity process. Similar to the governance structure depicted in Figure 3, departments should ensure that key representatives both from the functional and technical side of the organization are identified.

Output/Deliverable

The deliverable associated with this activity consists of a governance structure with key stakeholders identified at all levels of the organization.

2.3 Develop Business Continuity Plan

Process

The objective of the Business Continuity Plan activity is to provide the department's specific details regarding the implementation of this guide. It should answer the basic questions: what, who, when, how.

Note: Currently, departments have only been asked to develop risk management plans. These plans will need to be enhanced to include the other aspects of this revised guide.

Output/Deliverable

The deliverable to be developed as part of this task consists of a Business Continuity Plan which provides the department's specific details regarding the implementation of this guide. A sample table of contents is provided in Appendix A.

2.4 Obtain Commitment

Process

Business continuity issues will emerge well before the Year 2000 and members of the governance structure will need to be involved. The objective of the "Obtain Commitment" activity is to obtain the commitment of these stakeholders to support the process documented in the plan and to adapt to the needs of the department regarding timely decisions, strategic and policy directions, as well as oversight.

Output/Deliverable

The deliverable for this task is a revised or new project charter that clearly identifies the members of the governance structure and their roles and responsibilities regarding the business continuity process. One of the most important aspects of the new charter is the governance structure member's responsibility regarding their organization's response vis-à-vis certain risks. For example, members of the governance structure on the functional side of the organization should make the final decision regarding the development and activation of contingency plans.

The charter should include highlights of the business continuity plan including the resource commitments (human and financial) made to the business continuity process. A sample table of contents is provided in Appendix B.

2.5 Involve the Governance Structure

Process

The objective of the "Involve the Governance Structure" activity is to develop vehicles to ensure the continuous involvement of the governance structure members.

Ouput/Deliverable

The deliverables for this task include:

a. Monthly Steering Committee meetings;
b. Minutes of the monthly Steering Committee meetings with the attendance list;
c. Revised risk list;
d. Status reports; and
e. Revised plans.

2.6 Techniques and Tools

Table 2 provides a summary of the techniques and tools used for this step. Details of the techniques and tools can be found in the appendices or the referenced documents.

Table 2: Business Continuity Governance Structure Setup Techniques and Tools

Activity	Techniques and Tools
Setup the Governance	No specific tool
Develop Business Continuity Plan	Business Continuity Plan – Table of Contents (Appendix A)
Obtain Commitment	• Sample Project Charter (Appendix B)
Involve the Governance Structure	• Monthly Steering Committee meetings; • Minutes of the monthly Steering Committee meetings with the attendance list; • Revised risk list; • Status reports; and • Revised plans.

3
Identify

In order to initiate and feed the business continuity process with essential information, departments must identify those risks that may impact the achievements of the technical (compliance) and functional (business continuity) objectives. The absence of clear risk identification will lead to an unfocused business continuity process and the possible inability of departments to respond to crises.

3.1 Process

Note: This risk identification activity is based on the SEI "Identify" process [CRM Guidebook, Chapter 4, Page 27].

The objective of the risk identification step is to locate risks that may impact the ability of the department to convert their Year 2000 susceptible assets before they become problems and to ensure business continuity. The step includes the identification of risks through the use of a taxonomy questionnaire and the documentation of these risks in Risk Identification Sheets. That information will then be fed into the analysis phase where risk attributes will be defined and documented.

3.2 Data Flow

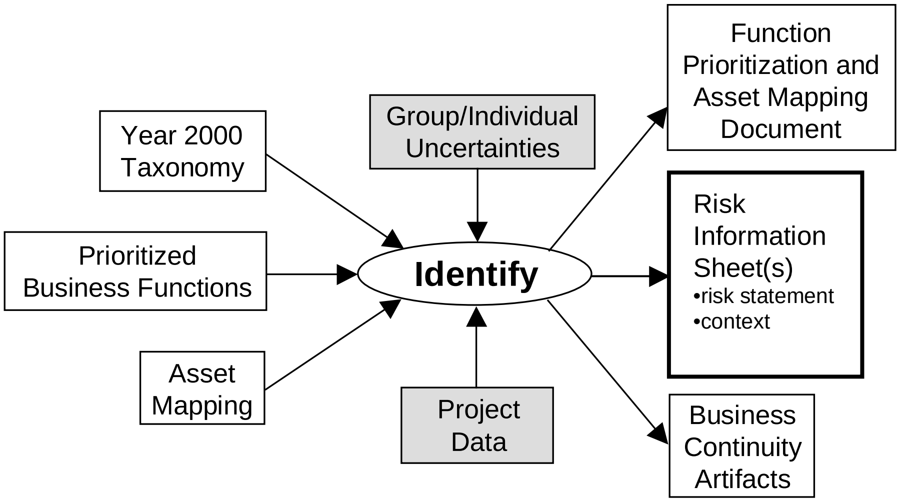

Year 2000 Taxonomy
Prioritized Business Functions
Asset Mapping
Group/Individual Uncertainties
Project Data
Identify
Function Prioritization and Asset Mapping Document
Risk Information Sheet(s)
•risk statement
•context
Business Continuity Artifacts

Figure 4 – Identify Data Flow

The following data inputs are required (shaded boxes is not included):

Input

Table 3: Identify Data Inputs

Data Input	Description
Year 2000 Taxonomy	The Year 2000 taxonomy is the main tool used to support risk identification. It consists of a series of questions that highlight important aspects of a Year 2000 project.
Prioritized Business Functions	A functional decomposition is primarily conducted to help identify risks by allowing participants to relate them to specific business functions (unless the risk is high level, affecting all aspects of the project). A prioritized list of business functions will assist in analyzing and ranking the risks or related business continuity activities.
Asset Mapping	Asset mapping is essentially a list of assets (susceptible or not) that support a specific business function. The asset mapping will help the risk identification activity by allowing participants to relate risks to specific assets (unless the risk is high level, affecting all aspects of the project).

Output/Deliverable

The deliverables for this task include:

a. A set of risk information sheet(s) that can be used to document each risk;
b. A function prioritization and asset mapping document; and
c. Business continuity artifacts, such as contingency plans, crisis response plans and business resumption plans.

3.3 Techniques and Tools

Table 4 provides a summary of the techniques and tools used for this step. Details of the techniques and tools can be found in the appendices or in the referenced documents.

Table 4: Identify Techniques and Tools

Activity	Techniques and Tools
Business Function Prioritization	• Functional Decomposition Approach (Appendix C) • Business Function Prioritization Approach (Appendix D) • Business Prioritization and Asset Mapping Document – Table of Contents (Appendix E)

Activity	Techniques and Tools
Asset Mapping	• Asset Mapping Approach (Appendix F) • Business Prioritization and Asset Mapping Document – Table of Contents (Appendix E)
Identify	• “Identify” Detailed Procedures (Appendix G); • Year 2000 Taxonomy (Appendix H); • Risk Information Sheet (Appendix I); and • Sample Risk List (Appendix J).
Identify Business Continuity Artifacts	• Sample Business Continuity Artifacts (Appendix K)

3.4 Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this step.

a. Involve all stakeholders in the risk identification step;
b. Involve the governance structure quickly because most organizations have not been adept at cross-functional business function prioritization and decisions will be required;
c. State risks in objective terms, making sure that there is a potential negative impact on the Year 2000 Project and/or business continuity objectives of the department;
d. Conduct periodic risk identification at the end of major milestones, phases or activities;
e. Identify owners for functions and assets. Function owners are responsible for the continuity of their functions. Assets owners are often those individuals that will be tasked to oversee/perform the conversion of these assets.
f. Ask business function owners to score their respective business functions against the TBS criticality criteria and obtain initial list. Use groups and pair-wise comparison techniques to finalize ranking;
g. Ensure that the risk statement and context information are clearly and objectively stated;
h. Use existing business models within the department as a starting point to developing a business model in support of this process;
i. Stay focused on the Year 2000 mission. The need is not for a perfect business model but for a list of business functions that can be associated to assets and can be assigned to specific individuals;
j. Coverage (i.e. all business functions) is more important than details (depth of the decomposition);
k. Let business function owners do the first asset mapping; use groups, including technical individuals, to validate the asset mapping;
l. Focus on asset mapping coverage first (identify as many assets as possible), refine as conversion progresses; and
m. Involve legal personnel to determine department’s liabilities.

4 Analyze

In order to make sound decisions regarding potential actions that will ensure business continuity, governance personnel must achieve a clear understanding of the department's exposure to risks and related business interruptions. Clearly defined risk attributes provide this required knowledge and can be acquired through analyzing the risks found in the previous step. A lack of understanding of the potential negative consequences of Year 2000 related risks may prevent departments from pro-actively dealing with potential crises and minimizing the impact on their programs and services.

4.1 Process

Note: Risk analysis is based on the SEI "Analyze" process [CRM Guidebook, Chapter 5, Page 37].

Departments must convert the risk information, gathered in the "identify" step, into decision-making information. In addition to defining the risk attributes such as probability, impact, timeframe, source, response and priority, departments must relate the risk information to assets and functions.

a. Probability: The likelihood that the risk will materialize;
b. Impact: The loss or impact on the Year 2000 Project and business continuity if the risk materializes;
c. Timeframe: The period in which the risk may materialize;
d. Source: The source of the risk;
e. Response: The department's response to the risk; and
f. Priority: The priority or rank of the risks within the department.

This analysis will allow departments to clearly understand the potential impact of risk on business continuity and to take the appropriate management actions to address the risks.

This information will be obtained through the use of workshops with technical and functional personnel and various other techniques identified herein. The analysis phase will also complement the risk analysis with a the definition of the business continuity requirements and the assessment of the department's capability in the area of business continuity.

4.2 Data Flow

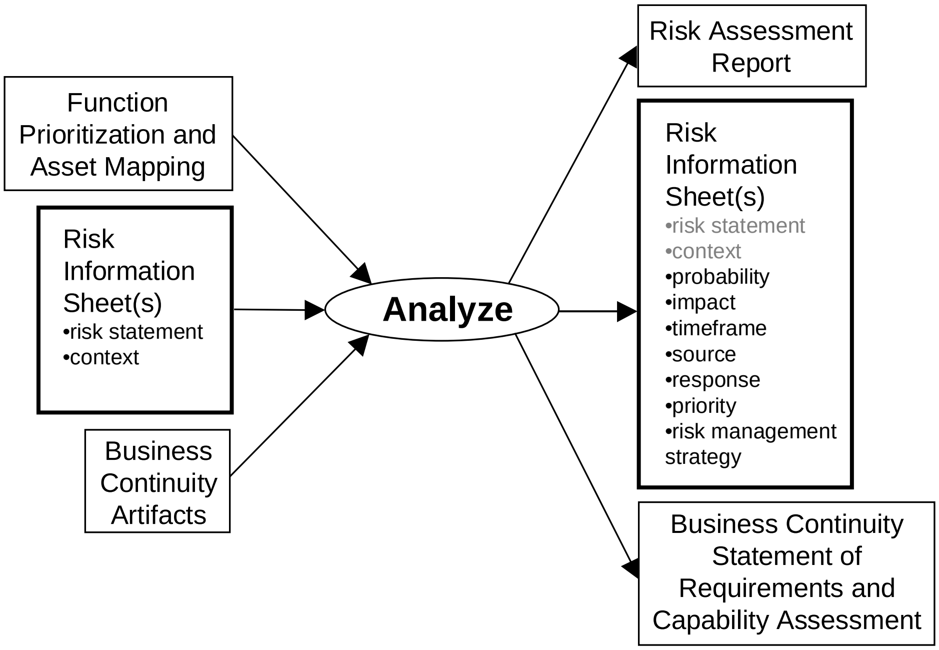

Function Prioritization and Asset Mapping
Risk Information Sheet(s)
•risk statement
•context
Business Continuity Artifacts
Analyze
Risk Assessment Report
Risk Information Sheet(s)
•risk statement
•context
•probability
•impact
•timeframe
•source
•response
•priority
•risk management strategy
Business Continuity Statement of Requirements and Capability Assessment

Figure 5 – Analyze Data Flow

The following data inputs are required:

Input

Table 5: Analyze Data Inputs

Data Input	Description
Risk Information Sheet(s)	Risk Information Sheets as defined in the “Identify” step including the risk statement and context.
Function Prioritization and Asset Mapping Document	Contains the prioritized business functions using pre-defined criticality criteria and maps mission-critical business functions to assets.
Business Continuity Artifacts	A list of business continuity artifacts such as existing business resumption plans and disaster recovery plans that should be used in support of the analysis function.

Output/Deliverable

The deliverables for this task include:

a) Risk information sheet(s) with risk attributes (probability, impact, timeframe, source, response, priority and risk management strategy);

b) Risk assessment report; and

c) Business continuity statement of requirements and capability assessment. This assessment should be a textual statement of the requirement for business continuity activities, based on the results of the risk analysis. It should also include an assessment of the department's capability to respond to business interruptions.

4.3 Techniques and Tools

Table 6 provides a summary of the techniques and tools used for this activity. Details of the techniques and tools can be found in the appendices or the referenced documents.

Table 6: Analyze Techniques and Tools

Activity	Techniques and Tools
Analyze	• "Analyze" Detailed Procedures (Appendix L) • Risk Information Sheet (Appendix I) • SEI Continuous Risk Management Taxonomy-based Questionnaire Interviews [Chapter A-33, page 495] • Tri-level Attribute Evaluation [CRM Guidebook, Chapter A-38, Page 521];
Risk Assessment	• Sample Risk Assessment Report – Table of Contents (Appendix M)
Business Continuity Statement of Requirements and Capability Assessment	• Business Continuity Requirements Definition Detailed Procedures (Appendix N)

4.4 Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this activity:

a) Combine risk identification and analysis activities in order to optimize participant's time;

b) Go qualitative first and support big risk items with more quantitative analyses;

c) Focus on "Top-N" risks;

d) Conduct the risk analysis in a workshop setting with Year 2000 Project key stakeholders in order to provide a department-wide view, particularly for the "response" attribute;

e) Acknowledge risks that have materialized and are now problems. This will provide sufficient exposure to ensure that these problems are dealt with.

f) Collect all types of documents that may contain business resumption elements such as standard operating procedures, operations manuals, maintenance procedures, etc.

5
Plan

In order to establish a yardstick against which a department's progress in implementing business continuity can be measured, plans must be developed and implemented. Failure to develop these plans may significantly affect the department's preparedness in dealing with possible crises.

5.1 Process

Note: Risk planning is based on the SEI "Plan" process [CRM Guidebook, Chapter 6, Page 53].

With the first three activities completed, departments can then develop plans to address the risks and ensure their preparedness to ensure business continuity. The two plans that need to be developed are:

a) **Risk Action Plan**. This plan will address known risks and develop specific strategies to address the risks; and

b) **Business Continuity Preparedness Plan**. This plan address all the components required to respond and recover from a crisis. It addresses both compliancy and business continuance contingency plans developed for specific risks or events; crisis scenarios to link possible risk events; crisis response plans, and business resumption plans.

These plans should be developed by members of the governance structure assigned to the areas of the business continuity process (i.e. risk action plan, contingency planning, crisis management, and business resumption).

The process to be implemented consists of providing the information identified in the corresponding templates and, more importantly, mobilizing the resources to implement the plans.

More specifically, the objective of the Risk Action Plans is to determine what actions should be taken, if any, to mitigate the identified risks. Risk action planning answers the following questions:

Table 7: Risk Action Planning Questions

Question	Explanation
- *Whose risk is it?*	Responsibility must be assigned for each risk item
- *What can be done about it?*	An approach or strategies to deal with the risk item must be developed
- *How much and what should be done?*	The scope and actions to manage the risks must be determined

The resulting risk action plans must then be implemented according to the assigned responsibilities.

The objective of the business continuity preparedness plan is to address all the components required to respond and recover from a crisis. In essence, it also answers fundamental questions such as:

Table 8: Business Continuity Planning Questions

Question	Explanation
- *Where are the risks? Where should we develop contingencies? What will be those contingencies?*	Departments must develop both compliance and business continuity contingency plans for those areas where they are exposed.
- *What are the likely crisis scenarios?*	Departments must attempt to anticipate likely crisis scenarios in order to develop effective responses to these events.
- *What needs to be done in order to recover from these crises?*	Departments must determine what needs to be done in order to revert back to normal operations after experiencing a crisis or implementing a contingency plan.

Both of these plans are supported by templates.

5.2 Data Flow

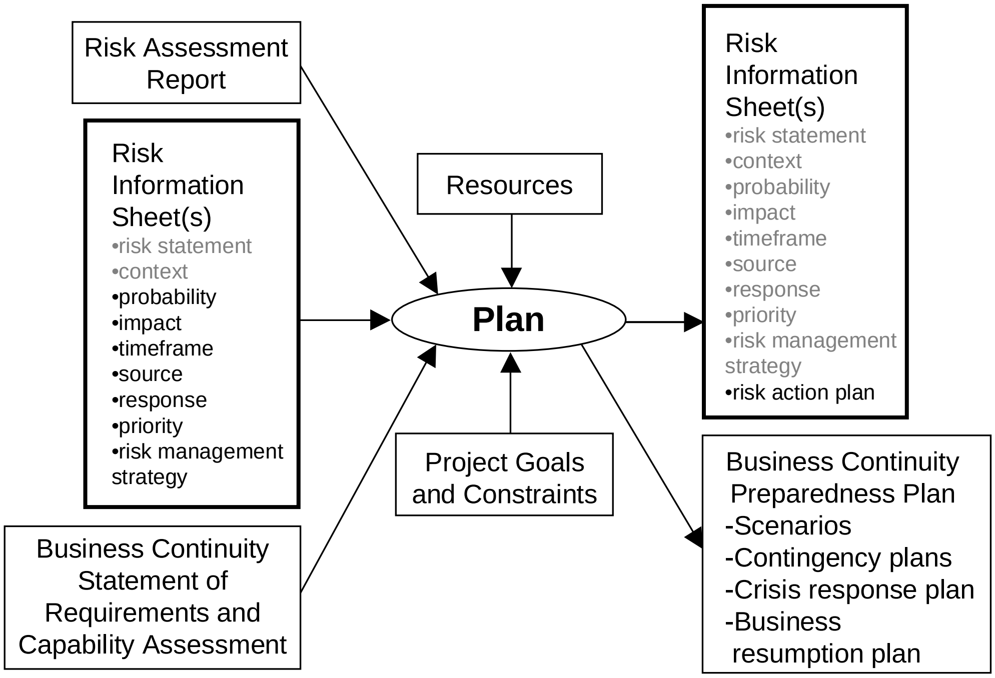

Risk Assessment Report
Risk Information Sheet(s)
•risk statement
•context
•probability
•impact
•timeframe
•source
•response
•priority
•risk management strategy
Business Continuity Statement of Requirements and Capability Assessment
Resources
Plan
Project Goals and Constraints
Risk Information Sheet(s)
•risk statement
•context
•probability
•impact
•timeframe
•source
•response
•priority
•risk management strategy
•risk action plan
Business Continuity Preparedness Plan
-Scenarios
-Contingency plans
-Crisis response plan
-Business resumption plan

Figure 6 – Plan Data Flow

The following data inputs are required:

Input

Table 9: Plan Data Inputs

Data Input	Description
Risk Information Sheet(s)	From the "Analyze" activity containing the risk information
Risk Assessment Report	Contains the risk information as well as other background information such as observations or problems.
Business Continuity Statement of Requirements and Capability Assessment	From the "Analyze" activity, stating the requirements for contingency planning.

Output/Deliverable

The deliverables to be developed as part of this task include:

a) Updated risk information sheet(s) with the risk action plan information; and
b) Business continuity preparedness plan, with crisis scenarios, contingency plans, crisis response plan and business resumption plan.

5.3 Tools and Techniques

Table 10 provides a summary of the techniques and tools used for this activity. Details of the techniques and tools can be found in the appendices.

Table 10: Plan Techniques and Tools

Activity	Techniques and Tools
Plan(s)	• "Plan" Detailed Procedures (Appendix O) • [CRM Guidebook, Chapter A-7, Page 295].
Develop Business Continuity Preparedness Plan	• Sample Contingency Planning – Table of Contents (Appendix P) • Crisis Scenario Definition Detailed Procedures (Appendix Q) • Sample Crisis Response Plan – Table of Contents (Appendix R) • Sample Business Resumption Plan – Table of Contents (Appendix S)

5.4 Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this activity.

a) Plan important risks first (those that are likely to materialize soon and have a significant negative impact);

b) Plan efficiently (stay focused on the cost-benefit of the proposed plans);

c) Ensure that the risk action plans address the source of the risk;

d) Make sure that key stakeholders are present and provide input into the planning process;

e) Implement the risk action plans in a timely manner in order to effectively deal with the risks;

f) Communicate the risk mitigation strategy and risk action plans (included as part of the updated Risk Information Sheets) to the Governance Structure members; and

g) The level of contingency planning should be commensurate to the level of exposure for each function (i.e. the more exposed a function is to disruption, the greater the efforts should be in the area of contingency planning).

6
Track

Departments must develop the capability to continuously assess risk and report on the progress of the business continuity plans and the conversion activities. Status reports emerging from this step will feed in the business continuity process and trigger the proper management actions such as activating contingency plans, declaring a crisis, or resuming a business function. Inadequate tracking may lead to ineffective actions or chaos that can disrupt operations.

6.1 Process

Note: Risk tracking is based on the SEI "Track" process [CRM Guidebook, Chapter 7, Page 73].

The tracking step aims at collecting progress information from the conversion activities and risk action plans and feeding issues and risks into the business continuity process. Other indicators that could activate contingencies or emergency responses should also be tracked. This will provide a disciplined environment that allows departments to:

- Continuously assess what could go wrong;
- Determine which risks are important to deal with and could negatively impact the continuity of the department's business; and
- Implement strategies to deal with those risks.

This step normally builds on existing reporting mechanisms such as project progress reporting, continuous risk management, verification and validation, as well as quality assurance. The objectives of the tracking step are two-fold:

a) First, departments must ensure that the plans, from the previous step, are implemented in accordance with the defined objectives; and
b) Secondly, departments must track problems and risks to trigger management actions and any other indicators that could activate contingencies or emergency responses.

6.2 Data Flow

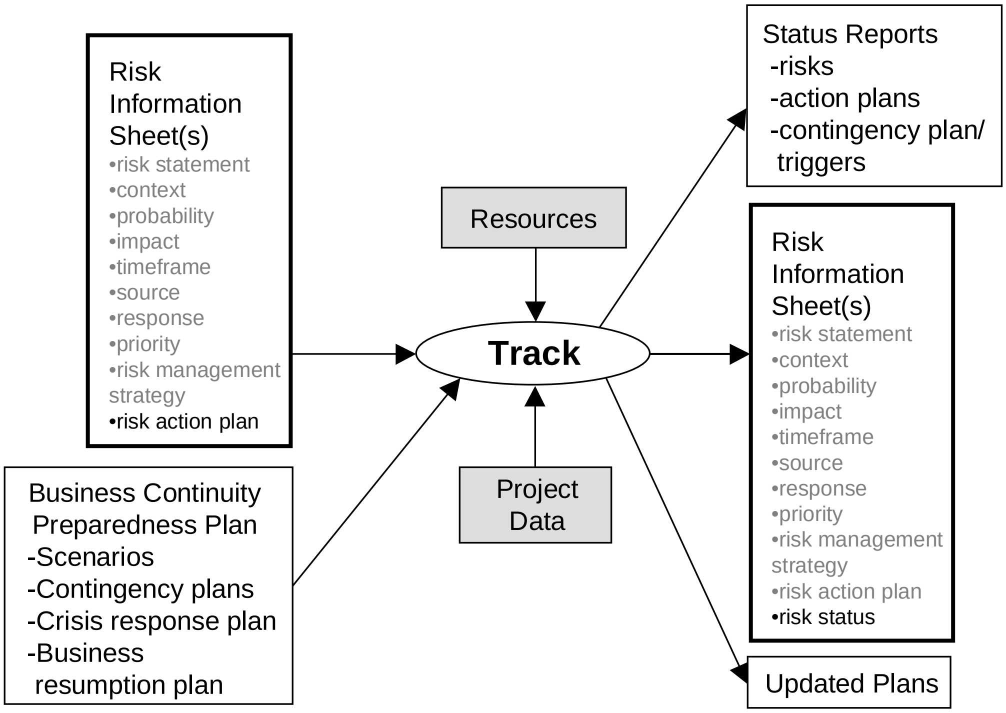


Figure 7 – Track Data Flow

The following data inputs are required (shaded items not included):

Input

Table 11: Track Data Inputs

Data Input	Description
Risk Information Sheet(s)	From the “Plan” activity, including the risk action plan.
Business Continuity Preparedness Plan	From the “Plan” activity, including the processes to be implemented.

Output/Deliverable

The deliverables to be developed as part of this task include:

a) Revised risk information sheet(s) with risk status;
b) Status reports (verbal and/or written); and
c) Updated plans.

6.3 Techniques and Tools

This table provides a summary of the techniques and tools used for this activity. Details of the techniques and tools are provided in the appendices or the referenced documents.

Table 12: Track Techniques and Tools

Activity	Techniques and Tools
Track	• "Track" Detailed Procedures (Appendix T) • Risk Information Sheets (Appendix I); • Risk Action Plan Implementation Tracking spreadsheet [CRM Guidebook, Chapter A-30, Page 461]; and • Risk status report – can use a format similar to the "Spreadsheet Risk Tracking" (similar concept to the Risk Action Plan Implementation Tracking spreadsheet) [CRM Guidebook, Chapter A-30, Page 461].

6.4 Guidelines and Tips

The following are general guidelines and tips regarding this step:

a) Establish effective data gathering by leveraging current data gathering activities within the Year 2000 projects;

b) Ensure that the implementation of risk action plans and the closing of risks are properly identified and documented;

c) Ensure timely reporting of the risk status and information; and

d) Use automated tools to track artifacts (plans, status reports, RIS, etc.) and key milestones.

7
Control

In response to variances in the plans or risk events, departments must initiate actions that will ultimately correct the situation and return the operations to their normal status. The control step addresses all of the process areas required to achieve this goal namely: contingency plans, crisis response and business resumption. The control step assumes an orderly and structured approach to recovering from a crisis. Unprepared departments are likely to prolong the crisis state and potentially face total failure of certain functions.

7.1 Process

Note: Business continuity control is based on the SEI “Control” process [CRM Guidebook, Chapter 8, Page 91].

The control step is closely related to the decision-making process found within the governance structure and primarily consists of activating pre-planned responses to predictable events and applying a structured decision-making framework to unforeseen events. The objective of the control step is to make informed, timely, and effective decisions regarding risks, failures and crises related to Year 2000 issues.

7.2 Data Flow

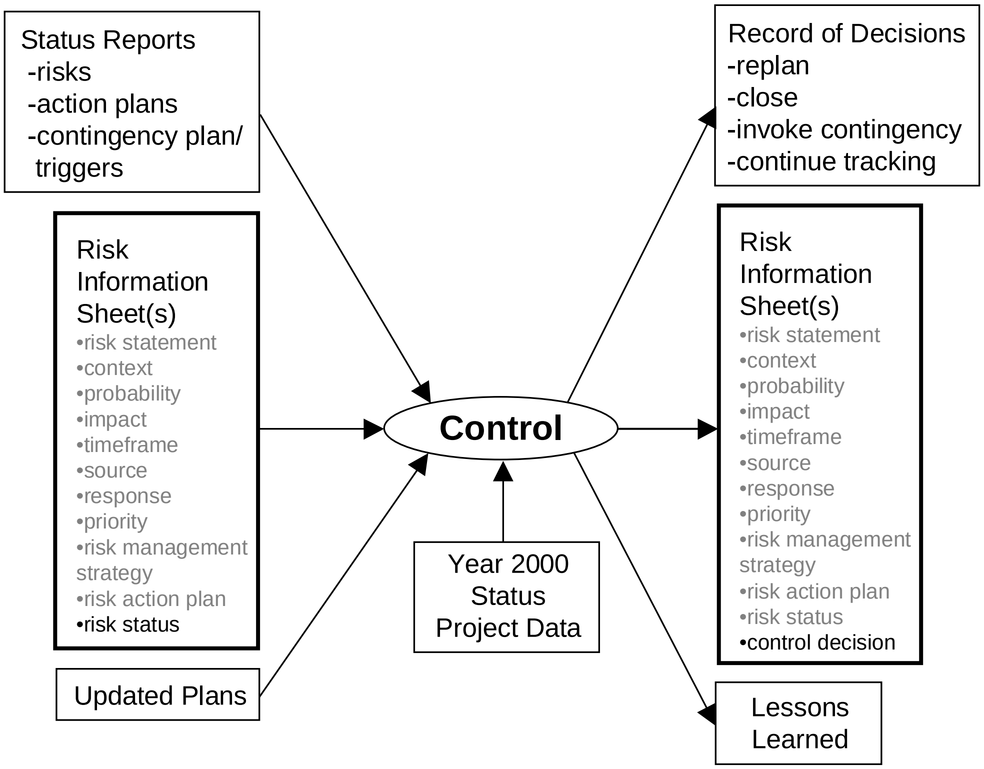


Figure 8 – Control Data Flow

The following data inputs are required:

Input

Table 13: Control Data Inputs

Data Input	Description
Status Reports	Contains status of business continuity plan implementation and status of risks.
Risk Information Sheet(s)	Developed during the previous activities, the sheets contain the risk status.
Updated Plans	Updated version of the plans defined in the “Plan” activity.

Output/Deliverable

The deliverables to be developed as part of this task include:

a) Record of decisions, including replan, close, invoke contingency or continue tracking;
b) Lessons learned; and
c) Updated risk information sheet(s), with control decision for risks.

7.3 Techniques and Tools

This table provides a summary of the techniques and tools used for this activity. Details of the techniques and tools can be found in the appendices.

Table 14: Control Techniques and Tools

Activity	Techniques and Tools
Control	- "Control" Detailed procedures (Appendix U); - Risk Information Sheets (Appendix I); - Risk status report – can use a format similar to the "Spreadsheet Risk Tracking" (similar concept to the Risk Action Plan Implementation Tracking spreadsheet) [CRM Guidebook, Chapter A-30, Page 461]; and - Cause and Effect Analysis [CRM Guidebook, Chapter A-8, Page 301].

7.4 Guidelines and Tips

The following are general guidelines and tips for effectively implementing this activity:

a) Make informed decisions based on the indicators/measures identified on the Risk Information Sheets;
b) Document lessons learned; and
c) Document the rationale for closing risks.

8
Concluding Remarks

8.1 Next Steps

This guide is only one of the methods used in increasing the government's capability of addressing the Year 2000 challenge and ensuring the continuance of its business mission-critical functions. The purpose of the guide is to encourage departments to implement a business continuity process within their organization. This document provides a framework that identifies the minimum set of activities that should be performed. Each department should now tailor the steps found herein and implement a business continuity process within their Year 2000 initiatives.

At the government level, TBS will now be in a better position to ensure that the government is ready to face the potential crises related to the Year 2000 problem and to assist departments in resolving horizontal issues and risks.

8.2 Conclusion

Implementing industry best practices such as those described in this guide offers departments an opportunity to embrace proven solutions which will enhance their ability to manage and deliver their Year 2000 projects while solving one of the government's biggest problems.

Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

APPENDICES to

Steering Government into the Next Millennium:

A Guide to Effective Business Continuity in Support of the Year 2000 Challenge

October 14, 1998
Enhanced Management Framework for IT
Chief Information Officer Branch
Treasury Board of Canada Secretariat

Canada

PUBLICATION HISTORY

Version	Release Date	Revisions
0.1	June 15, 1998	Second Draft for TBS review only.
0.2	June 18, 1998	Draft for distribution to Translator.
1.0	June 19, 1998	Draft for distribution to departments at June 22, 1998 meeting.
1.1	June 26, 1998	Final with TBS comments incorporated.
2.0	September 29, 1998	Second version for review
2.1	October 14, 1998	Final version

TABLE OF CONTENTS

LIST OF APPENDICES

Preface

Background

The Canadian federal government, like most public and private sector organizations will be facing a problem when the year changes from 1999 to 2000.[3] Many systems that use a date in their processing, have traditionally utilized the date as a two-digit reference instead of a four-digit reference. The change to a new millennium may result in an error in date-related processing unless changes are made to these systems.

The potential negative consequences of the Year 2000 problem are far reaching and could bring entire organizations to a halt, or at least significantly impact their ability to deliver their services or products. Within the context of the federal government, the consequences could have highly undesirable impacts on Canadians, the country, and its economy. Specifically, these problems relate to inaccurate date processing or “denial of government service” issues when the systems crash.

The Treasury Board of Canada Secretariat (TBS) has initiated a project to address the Year 2000 problem across the government. A Project Office was established to initiate activity and to facilitate and monitor the progress on converting assets supporting government-wide mission-critical functions. A preliminary assessment of the significance of the Year 2000 problem across the government determined that 48 government-wide mission-critical functions might be sensitive to this problem.

The latest readiness assessment[4] of the government’s progress in solving the Year 2000 problem shows that there is still a significant amount of work to be completed before the year 2000. The current project status suggests that government departments must consider the possibility that government services and programs will be affected by Year 2000 failures. Within that context, TBS is taking a leadership role in advising departments to:

a. Assess what could go wrong;
b. Develop contingency plans as required;
c. Ensure that departments have in place the proper framework to manage crises related to Year 2000 and associated events; and
d. Plan for full business resumption, following a Year 2000 related business interruption.

Specifically, TBS is providing departments with this guide to business continuity, which will enhance the government’s ability to address the potential negative consequences of the Year 2000 problem.

[3] There is also a related issue about leap year processing from the “extra” leap year for Feb 29, 2000.
[4] Braiter/Westcott Report on Year 2000 Readiness, February 1998.

Why this Guide was Developed

This guide was developed to:

a. Help departments manage risks associated with their Year 2000 initiatives, and ensure uninterrupted and fully functional delivery of programs and services to Canadians in spite of Year 2000 related failures;

b. Help departments identify business continuity issues and properly prepare to manage Year 2000 problem related crises; and

c. Help the TBS ensure that departments are ready to face the potential negative consequences of the Year 2000 problem and that the government is aware of the risks and consequences associated with not solving the Year 2000 problem.

Purpose of this Guide

The purpose of this document is to present a uniform and standardized set of business continuity activities for all departments to implement in order to facilitate the government's governance of the Year 2000 problem and thereby increase its likelihood of success.

Acknowledgment

TBS would like to acknowledge the contributions of the following participants:

a. ***Godcharles Goulet Fournier Consulting Inc.*** for developing this guide;

b. Veterans Affairs Canada for initiating the process;

c. The Software Engineering Institute, for allowing us to use their risk management material;

d. The departments of Fisheries and Oceans Canada, Agriculture and Agri-Food Canada, Public Works and Government Services Canada and Human Resources Development Canada for sharing some of their process artifacts; and

e. Magellan Engineering Consultants Inc. for their contribution in the areas of crisis response and business resumption.

Appendix A
Sample Business Continuity Plan – Table of Contents

The business continuity plan should include, as a minimum, but not be limited to the following elements:

EXECUTIVE SUMMARY

1. INTRODUCTION
Positions the Business Continuity guide in the departmental Year 2000 initiative.

1.1 Background
1.2 Objective
1.3 Scope
1.4 Business Continuity Process Overview (summary of this guide)
1.5 References

2. BUSINESS CONTINUITY PROCESS AREAS
Summarizes department’s approach in implementing the various process areas of the guide.

2.1 Continuous Risk Management
2.2 Contingency Planning
2.3 Crisis Response
2.4 Business Resumption

3. ORGANIZATION AND RESPONSIBILITIES
Identifies key stakeholders involved in the implementation of the Guide along with their roles and responsibilities. (Responsibility Assignment Matrix).

3.1 Governance Structure
3.2 Key Year 2000 Business Continuity Stakeholders’ Responsibilities
3.3 Business Continuity Governance Framework
3.3.1 Meetings
3.3.2 Communications

4. METHODS, TECHNIQUES AND TOOLS
Identifies the methods, techniques and tools selected by the department to support the process.

4.1 TBS Business Continuity Tailoring Matrix
4.2 Plan Maintenance

Appendix B
Sample Project Charter – Table of Contents

The project charter should include, as a minimum, but not be limited to the following elements:

EXECUTIVE SUMMARY

1. INTRODUCTION
    1.1 Background
    1.2 Objective
    1.3 Scope
    1.4 References

2. APPROACH OVERVIEW
    2.1 Business Continuity Activities
    2.2 Implementation Overview
    2.3 Key Milestones

3. ORGANIZATION AND RESPONSIBILITIES
    3.1 Governance Structure
    3.2 Key Year 2000 Business Continuity Stakeholders' Responsibilities
    3.3 Business Continuity Governance Framework
        3.3.1 Meetings
        3.3.2 Communications

4. RESOURCE REQUIREMENTS
    4.1 Human Resource Requirements
    4.2 Financial Resource Requirements
    4.3 Other Resource requirements

5. SIGN-OFFS

Appendix C
Functional Decomposition Approach

1. How to Decompose an Organization's Main Function into a Business Model

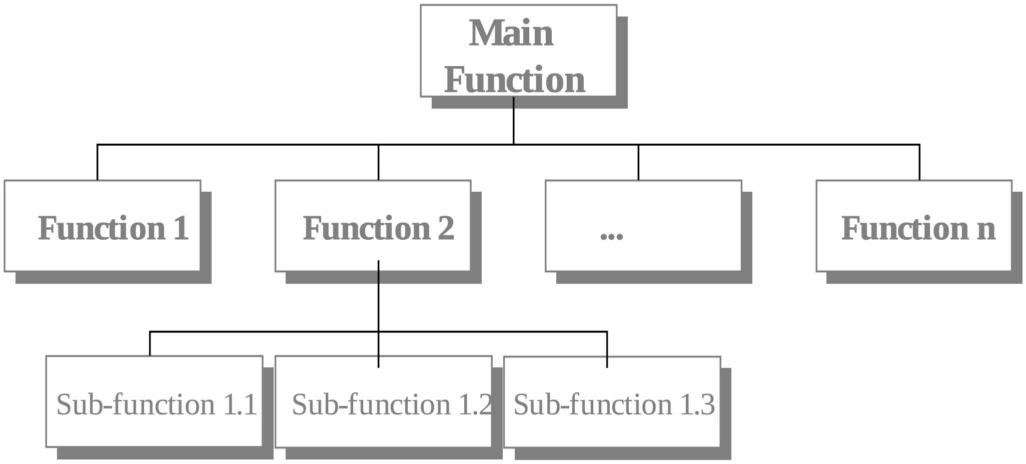
To support the business continuity process, departments must develop a business model that accurately and uniquely identifies all the functions performed by the organization. These functions should be depicted in a tree-like fashion to reflect the hierarchical relationship between these functions (indented models can also be used).

2. Develop a Business Model

2.1 Process

The objective of this process is to conduct a functional decomposition of the department's main function into sub-functions to the point where single ownership can be assigned (see additional guidelines & tips for more direction).

2.2 Deliverable



The deliverable to be developed as part of this task is a business model or functional decomposition which accurately identifies all the functions performed by the organization and depicts them in a tree-like fashion to reflect the hierarchical relationship between these functions. A sample is provided below.

Figure C-1 – Sample Functional Decomposition

3. Techniques and Tools

This table provides a summary of the techniques and tools used for this activity. Details of the techniques and tools can be found in the referenced documents.

Table C-1: Functional Decomposition Techniques and Tools

Activity	Techniques and Tools
Perform Functional Decomposition	No specific tool required. This technique can be found in many system development and business modeling methodologies.

4. Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this activity.

a. Functions consist of “actions” or “activities” that are part of a process used to deliver a service or a product (e.g. collect data, analyze data, and produce report);
b. Functions are usually described with a verb and a complement (e.g. pay employee, deliver benefit, etc.);
c. The functional decomposition process will refine the main functions of the department into sub-functions. To do so, it often uses the organizational structure to guide the decomposition of the main function into its lowest practical level of decomposition (i.e. look at the organizational chart to do your decomposition);
d. For many departments, the lowest practical level of functional decomposition will consist of these functions were single accountability can be assigned, and where all sub-functions (children) to a parent function use the same assets (i.e. when you determine that the next level of decomposition defines functions that all use the same assets, you stop at that level). Another indicator for the lowest practical level is when the criticality (impact of a given function on the operations of the government or the department) of all the sub-functions is all equal to the parent function;
e. Use existing business models within the department;
f. Stay focused on the Year 2000 mission, the need is not for a perfect business model but for a list of functions that can be associated to assets and can be assigned to one individual/organization;
g. Coverage (i.e. all functions) is more important than details (depth of decomposition); and
h. Involve the governance structure quickly to approve the functional decomposition.

Appendix D
Business Function Prioritization Approach

1. How to Prioritize Business Functions

To prioritize business functions, departments must utilize a business model that accurately identifies all the functions performed by the organization (Appendix C - Functional decomposition approach). Once assigned a unique function identifier, business functions can then be prioritized using pre-determined criteria. Within the context of the Year 2000 Project, these criteria should be those provided by TBS to determine the "mission-criticality" of specific government functions (i.e. when using the TBS criteria, the higher the function scores the more "mission-critical" it is).

2. Score Business Functions

2.1 Process

The prioritization process consists of scoring functions, found at the lowest level of the business model, based on the TBS criticality criteria and developing a prioritized list of functions that will provide the required framework to structure and sequence business continuity activities.

The total score of a given function is achieved as follows:

a. using the criteria found in Section D-1, functions should be scored against each criteria on the basis of their ability to have the identified impact. For example, the function "Pay employee" may score low on the criteria dealing with safety and environment but would score higher on economic well being of Canadians and employee morale;

b. the proposed scale to score each function against the criteria is as follows:

Low = 1	Medium = 3	High = 5

2 and 4 are used as intermediate values. 0 is used when the function does not have an impact in this area (Impact on safety, environment, etc.).

c. to score a function, individuals should ask themselves: "Is the impact's likelihood for a given function low, medium, or high? They would then assign a score from 1 to 5 based on their best judgement (this approach respects the risk concepts because the weighting factor represents the impact and the scores the probability); and

d. the weighting factors are applied to the total score achieved by a function in a given category. For example, if the total score of a function in the "Impact on Canadians" category is 25, this score would be multiplied by 5 to include the weighting factor assigned to this category. The scores from each category of criteria are then added to obtain the overall score for a given function.

2.2 Deliverable

The deliverable for this activity is a prioritized list of business functions.

3. Techniques and Tools

This table provides a summary of the techniques and tools used for this activity. Details of the techniques and tools can be found in the appropriate sections.

Table D-1: Business Function Prioritization Techniques and Tools

Activity	Techniques and Tools
Score Business Functions	• TBS Criteria – See Section D-1 in this Appendix • Sample Prioritized Function List – See Section D-2 in this Appendix

4. Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this activity.

a. Get function owners to score their respective functions against criteria, use groups to confirm the final ranking;
b. Use workshops with all functional areas to achieve the final list; and
c. Involve the governance structure quickly, as most organizations have not been culturally good at doing cross-functional business function prioritization, to make decisions.

Section D-1: TBS Criteria

The following table summarizes the criteria used to assess business functions as defined by the Treasury Board of Canada Secretariat. Weighting factors from 5 (High) to 1 (Low).

Table D-2 – Mission-critical Criteria

Criteria	Weight	Definition
Impact on Canadians	5	These criteria lead to the establishment of a government-wide mission-critical function. A government-wide mission-critical function has been defined as a service or function performed by a federal government department or agency:
		a. Which directly impacts the health, safety, security, or economic well-being of Canadians or their environment; and b. the loss or interruption of which, even for a short period, is deemed to be an unacceptable risk (recognizing that a Year 2000 failure is likely to take weeks or months to repair). *Note: Where these criteria should be applied to business functions, it has been decided that financial systems will be deemed government-wide mission-critical.*
• Health		Impact on the health/environment of Canadians. Sample business functions associated with this criteria include food inspection, drug management and testing, and other related functions from the "Health Canada" portfolio.
• Safety		Impact on the safety of Canadians. Sample business functions associated with that criteria include search and rescue functions.
• Security		Impact on the security of Canadians. Sample business functions associated with that criteria include law enforcement, correctional services, and other related functions from the Solicitor General's portfolio. Defence related functions are also associated with this criteria.
• Economic well being		Impact on the economic circumstance of Canadians. Sample business functions associated with that criteria include Receiver

Criteria	Weight	Definition
		General functions, Pension, Welfare, and other functions that provide economical benefits to Canadians.
• Environment		Impact on the environment of Canadians and Canada. Sample business functions associated with that criteria reside within Environment Canada, environmental response groups in Fisheries and Oceans.
Impact on Obligations	3	These criteria lead to the establishment of a department-wide mission-critical function. Within the context of this guide, a department-wide mission-critical function has been defined as a service or function performed by a federal government department or agency:
		a. Which will impact a department's service levels, contractual obligations with third parties, obligation to obey the law, regulatory obligations, and their obligations to other government departments, other levels of government, and/or foreign governments; and
		b. that the loss or interruption of which, even for a short period, is deemed to be an unacceptable risk.
• Service levels		Self-explanatory
• Contracts		Self-explanatory
• Legal/ Regulatory		Self-explanatory
• To other government departments		Within the Federal government.
• to other levels of government		Provincial, Regional, Municipal governments.
• to foreign governments		Self-explanatory
Impact on Employees	1	
• Workload/ ability to cope		Self-explanatory
• Morale/Stress		Self-explanatory
• Union		Self-explanatory
Financial Impact	1	

Criteria	Weight	Definition
• On government		Impact on Federal government where revenue or operating expenditure is affected, or cost is increased.
• on others		Self-explanatory

Section D-2: Sample Prioritized Function List

ID	Code	Function Name	Relative Score	Raw Score	Category
5.1.2	SAR	Detection of distress alerts	1	169	GWMC
5.1.5	SAR	SAR coordination	0.99	168	GWMC
5.1.4	SAR	Search and rescue planning	0.98	166	GWMC
3.1.1	MCTS	Detect and respond safety/distress calls	0.94	159	GWMC
3.1.2	MCTS	Respond to calls	0.94	159	GWMC
3.1.3	MCTS	Analyze situation	0.94	159	GWMC
3.1.4	MCTS	Alert proper agencies	0.94	159	GWMC
3.1.5	MCTS	Coordinate information process	0.94	159	GWMC
3.1.8	MCTS	Receive safety information from outside sources	0.94	159	GWMC
3.1.9	MCTS	Broadcast safety information	0.94	159	GWMC
5.1.1	SAR	Ensure SAR coverage by resources	0.82	139	GWMC
2.2.2	MNS	Provide electronic aids to navigation	0.80	135	GWMC
5.2.2	SAR	Environmental response operations	0.79	133	GWMC
5.3.2	ER	ER contingency planning exercising	0.79	133	GWMC
2.1.3	MNS	Overflow output/forecast/control	0.77	130	GWMC
2.1.4	MNS	Water level forecasting	0.77	130	GWMC
4.2.2	ICE	Ice routing and ice charts/info	0.77	130	GWMC
4.4.1	ICE	Monitoring of ice conditions	0.77	130	GWMC
4.4.2	ICE	Icebreaking for flood control	0.77	130	GWMC

Appendix E
Sample Business Prioritization and Asset Mapping Document – Table of Contents

The Business Prioritization and Asset Mapping Document should include, as a minimum, but not be limited to the following elements:

EXECUTIVE SUMMARY

1. INTRODUCTION
   - 1.1 Background
   - 1.2 Purpose
   - 1.3 Scope
   - 1.4 Definitions
   - 1.5 References

2. METHODOLOGY

3. BUSINESS FUNCTION PRIORITIZATION RESULTS
   - 3.1 Observations
   - 3.2 Overview Results

4. ASSET MAPPING RESULTS
   - 4.1 Observations
   - 4.2 Overview Results

<u>APPENDICES:</u>

Appendix 1 – Criticality Criteria
Appendix 2 – Functional Decomposition Results
Appendix 3 – Prioritized Business Function List
Appendix 4 – Asset Mapping Results

Appendix F
Asset Mapping Approach

1. How to Map Assets to Business Functions

In order to clearly link the asset conversion work to the business continuity activities, departments must map their Year 2000 assets to each function. This mapping provides a more detailed understanding of the relationship between risks related to the asset conversion work and the business risks and related impacts.

2. Map Assets to Business Functions

2.1 Process

The objective of this process is to map assets to the specific function they are supporting. Categories of assets should be developed in order to facilitate the mapping process. Recommended categories include:

a. Software (includes third party vendor software, operating systems, applications, etc.);
b. Networks (includes all equipment between the communication card on the end-terminals – LAN, MAN, WAN, PBX - including private switching equipment but excluding processing units such as PC's, servers, mainframes);
c. Real property systems (includes electrical supply, security, climate control, elevators and other systems);
d. Other organizations (includes other governments, departments, or organizations including these organizations that are part of the supply chain of the departments as well as the procurement and legal organizations);
e. Hardware (includes processing units such as PC's, servers, mainframes);
f. Utilities (includes electricity, telephone, mail service, etc.);
g. Fleets (includes aircraft, ships, automobiles, etc.); and
h. Embedded systems (includes manufacturing and process control; transportation and navigation equipment such as airplanes, trains, marine, traffic lights, air traffic control, etc.; office systems and mobile equipment such as faxes, copiers, videos, televisions, cell phones etc.; medical devices such as pacemakers, monitoring systems, x-rays, etc.; lab equipment).

2.2 Deliverable

The deliverable to be produced as part of this process is a "cause-and-effect" diagram as shown below. Using the cause-and-effect relationship between assets and business functions, departments can link their conversion activities to the business function they support. A sample "cause-and-effect" diagram, using the above categories, is provided below.

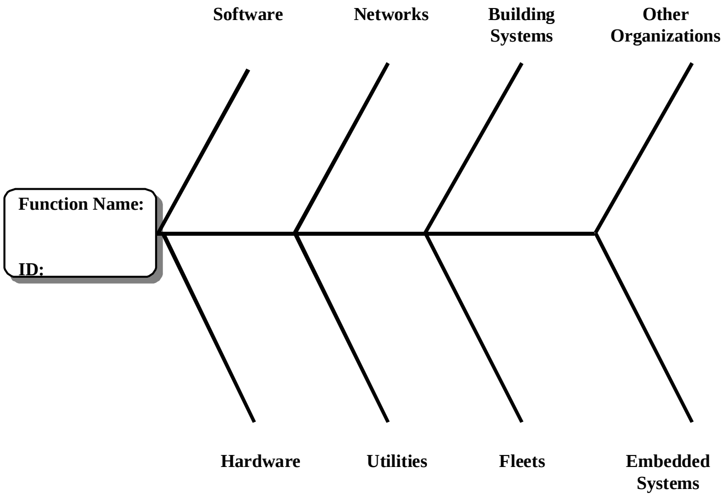


Figure F-1 – “Cause-and-effect” diagram

3. Document Asset Mappings

3.1 Process

The objective of this process is to document, in a clear and concise, fashion the results of the asset mapping exercise done using the “cause-and-effect” diagrams described in Section 2 above.

3.2 Deliverable

The deliverable to be developed as part of this activity is a table that identifies:

a. The name of the function;
b. The owner of the business function (including the phone number); and
c. The assets identified within each of the categories (Software, networks, building systems, other organizations, hardware, utilities, fleets, and embedded systems).

4. Techniques and Tools

This table provides a summary of the techniques and tools used for this process. Details of the techniques and tools can be found in the appendices or the referenced documents.

Table F-1: Asset Mapping Techniques and Tools

Activity	Techniques and Tools
Map Assets to Business Functions	Cause-and-effect Analysis [CRM Guidebook, Chapter A-8, Page 301].
Document Asset Mappings	A sample asset mapping table is provided in Section F-1 of this Appendix.

5. Guidelines and Tips

The following are guidelines and tips that can facilitate the performance of this activity:

a. Let function owners do the first mapping, use groups including technical individuals to validate the "cause-and-effect" diagrams produced by the function owners;

b. Focus on coverage first (identify as many as possible), refine as conversion progresses; and

c. Identify asset owners or asset category owners. Assets owners are often those individuals that will likely be tasked to oversee the conversion of these assets.

Section F-1: Sample Asset Mapping Table

The following asset mapping table is provided as an example only. It depicts the asset categories from Figure F-1 as column headings, and contains detailed assets for a specific business function.

Table F-2: Sample Asset Mapping Table

ID	Function Name	Software	Hardware	Networks	Utilities	Building Systems	Fleets	Other Branches/ Departments	Other Causes
5.1.2	Detection of distress alerts ("function owner")	- Detection EPIRB - Cospas-Sarsat Program at RCCs (DND) - Telex programs (Unitel)		- Cospas-Sarsat Datalink (telco - DND Authority) - PSTN (phone and telex) - Centrex SAR - CCG Net - National Cellulars communications Network	- Power/ Utilities	- RCC's (DND) - MRSC's (CCG)		- MCTS - Cospas-Sarsat Missions control centre - GTIS (centrex, long distance) - Inmarsat (Stratus)	- Other comms systems (need to raise flag on this issue)
5.1.5	SAR co-ordination ("function owner")	- Telex programs at RCC (telco) - RCC Databases (DND)	- RCC/ MRSC recording compo-nents	- PSTN (phone and telex) - Centrex SAR - CCG Net - National Cellulars communications Network	- Power/ Utilities	- RCC's - MRSC's		- ROCC - CG Regional Operations Centers - MCTS Centers - DND Vessels - MTSS - MSAT - Inmarsat	

ID	Function Name	Software	Hardware	Networks	Utilities	Building Systems	Fleets	Other Branches/ Departments	Other Causes
5.1.4	Search and rescue planning ("function owner")	- Cdn SAR Planning program - Search-master Program (DND) Rolled out - RCC/ MRSC's Databases	- RCC W/S platform (DND)	- Internet - DND Network - PSTN	- Power/ Utilities	- RCC's - MRSC's		**- Environment Canada Meteorolo-gical Centers** - MCTS (Vessel positioning)	

Appendix G
"Identify" Detailed Procedures

Process Overview

Risk identification can occur periodically at specified milestones/phases in a project and/or on a continuous basis throughout the project. The following table provides steps to identify risks under both scenarios.

Table G-1 – Risk Identification at specified milestones/phases

Risk Identification Steps	Description	Responsibility
1. Identify workshop/ interview participants	The Year 2000 Project Manager should determine the number of "peer-level" workshops with various stakeholder groups involved in the Year 2000 Project that is required to identify risks. Typical groups include: • Year 2000 Project Office (PO) personnel; • Year 2000 Steering Committee; • Year 2000 business function owners; • Year 2000 asset owners; • Technical leaders, asset conversion team members, infrastructure and communications resources; and • Regional representatives. The Year 2000 Project Manager should also establish the number of interviews with various executives involved in the Year 2000 Project required to complement the workshops. Typical interviews include: • Year 2000 Project Sponsor; and • Key governance structure members.	Year 2000 Project Manager
2. Schedule the risk identification workshops/ interviews	Generally, a risk identification workshop requires 3 hours to conduct and an interview anywhere from ½ hour to 2 hours. Workshops and interviews should all be scheduled before starting the process.	Year 2000 Project Manager
3. Tailor the TBS Risk Taxonomy questionnaire	The TBS Risk Taxonomy questionnaire (refer to Appendix H) should be tailored to reflect the subject areas of the workshop/interview participants as well as to meet the workshop/interview duration.	Year 2000 Project Manager

Risk Identification Steps	Description	Responsibility
4. Conduct the risk identification workshops/ interviews	Conducting the risk identification workshops/interviews involves: • Presenting an overview of the risk assessment (identification and analysis) process and its contribution to the business continuity process; • Reviewing and discussing each TBS Risk Management Taxonomy-based question or a subset(Appendix H), in order to identify risk areas (displaying the question on an overhead is a practical way of administering the questionnaire); and • Writing down notes from the discussion and documenting risk areas as they are identified.	Year 2000 Project Manager
5. Develop a risk list	Using the notes from the workshops/ interviews, look for common risk areas or consensus across various groups/ interviewees and develop a risk list. Each risk identified requires: • A statement of the risk which is comprised of a “condition” for the risk to exist as well as the “consequence” of the risk with respect to the business continuity objectives; and • A context of the risk which is intended to provide additional information about the risk. Risks should then be documented on a Risk Identification Sheet (Appendix I).	Year 2000 Project Manager

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.

Table G-2 - Continuous Risk Identification Steps

Risk Identification Steps	Description	Responsibility
1. Create a Risk Information Sheets	Any individual can identify a new risk by using the Risk Information Sheets (Appendix I). Each risk identified requires: • A statement of the risk which is comprised of a "condition" for the risk to exist as well as the "consequence" of the risk with respect to the business continuity objectives; and • A context of the risk which is intended to provide additional information about the risk.	Year 2000 Project stakeholder (programmer, tester, application manager, functional resources, etc.)
2. Review the Risk	The risk information sheets should then be forwarded to the Year 2000 Project Office for initial review.	Year 2000 Project stakeholder (programmer, tester, application manager, functional resources, etc.)
3. Forward the Risk Information Sheet to the Risk Owner and affected functions	Upon review and validation, the Project Office should then forward the risk to its owner for action planning as well as the function owners affected by the risk (if not the same person) in order to potentially trigger contingency plans.	Year 2000 project Office

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.

Appendix H
Year 2000 Risk Taxonomy

1. Introduction

1.1 Background

The Treasury Board of Canada Secretariat (TBS) Year 2000 Project Office requires that Federal Departments and Agencies with Government-Wide Mission-Critical (GWMC) business functions identify, report and manage Year 2000 project risks.

In order to provide guidance for identifying Year 2000 project risks, this Year 2000 Taxonomy provides for a comprehensive and structured classification scheme. Standard use of the TBS Year 2000 Taxonomy will provide for a common basis across departments for risk identification.

1.2 Purpose

The purpose of this appendix is to describe and document the TBS Year 2000 Taxonomy that can be used by Federal Departments in identifying the Year 2000 project risks associated with the Government-Wide Mission-Critical (GWMC) and Department-Wide Mission-Critical (DWMC) business functions. Departments may use their own taxonomy, but must ensure that all risk areas identified in the TBS Year 2000 taxonomy are addressed.

1.3 Scope

This appendix includes a description of “How to use the Year 2000 Taxonomy”, the Year 2000 Taxonomy questionnaire, a description of the Year 2000 Taxonomy questionnaire template data elements, and tips for using the Year 2000 Taxonomy.

1.4 Relationship to Other Documents

This document relates to the following documents as identified

a. Treasury Board of Canada Secretariat, Steering government into the next millennium: A Guide to Effective Business Continuity in Support of the Year 2000 Problem, October 1998.

b. Software Engineering Institute, Continuous Risk Management Guide, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1996.

The Year 2000 Taxonomy follows the principles of the Software Engineering Institute’s (SEI) Continuous Risk Management Guide, in particular the appendices regarding “Taxonomy-Based Questionnaire (Appendix A-32) and “Taxonomy-Based Questionnaire (TBQ) Interviews (Appendix A-33).

c. Treasury Board of Canada Secretariat, Year 2000 Risk Information Sheet (RIS), October 1998.

The Year 2000 RIS is the means for documenting information about risks that are identified as a result of conducting a risk assessment using the Year 2000 Taxonomy. A sample RIS is provided in Appendix I.

d. U.S. General Accounting Office’s, Year 2000 Computing Crisis, GAO/AIMD-10.1.14, September 1997.

The Year 2000 Taxonomy has been verified for completeness against the GAO Year 2000 Program Assessment Checklist.

e. Department of Information Technology, California 2000 Program Guide, State of California, November 1996.

The Year 2000 Taxonomy has been verified for completeness against the State of California's Year 2000 Project Approach, California 2000 Program Guide.

f. TBS, Year 2000 Mission Critical Contingency Planning Guide, Draft, April 1998.

The Year 2000 Taxonomy has been verified for against the survey questions found in the TBS Year 2000 Mission Critical Contingency Planning Guide.

g. The MITRE Corporation, Year 2000 Certification Process, http://www.mitre.org/research/y2k/docs.

The Year 2000 Taxonomy has been verified for completeness against the MITRE Corporation's Year 2000 Certification Process.

1.5 Glossary

The following glossary is intended to clarify certain terminology contained in the Year 2000 taxonomy.

- Asset: This refers to all items which may be impacted by the Year 2000 problem such as:
  - Software (includes third party vendor software, operating systems, applications, etc.);
  - Networks (includes all equipment between the communication card on the end-terminals – LAN, MAN, WAN, PBX – including private switching equipment but excluding processing units such as PC's, servers and mainframes);
  - Real property systems (includes electrical supply, security, climate control, elevators and other systems);
  - Other organizations (includes other governments, departments, or organizations including these organizations that are part of the supply chain of the departments as well as the procurement and legal organizations);
  - Hardware (includes processing units such as PC's, servers and mainframes);
  - Utilities (includes electricity, telephone, mail service, etc.);
  - Fleets (includes aircraft, ships, automobiles, etc.); and
  - Embedded systems (includes manufacturing and process control; transportation and navigation equipment such as airplanes, trains, marine, traffic lights, air traffic control, etc.; office systems and mobile equipment such as faxes, copiers, videos, televisions, cell phones etc.; medical devices such as pacemakers, monitoring systems, x-rays, etc.; and lab equipment).

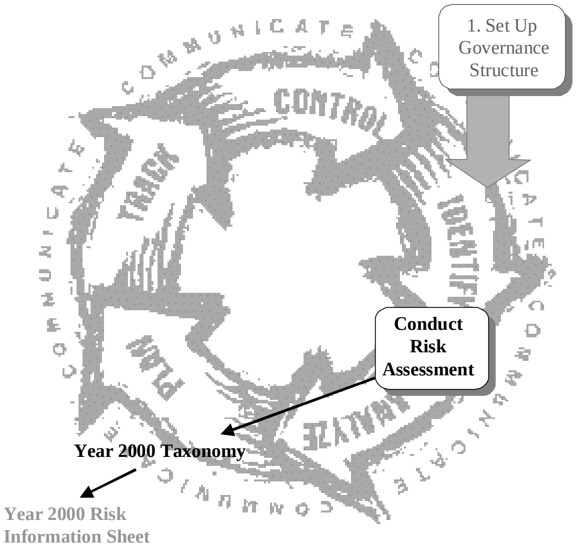
- Mission-critical business functions: Mission-critical business functions consist of specific business functions that have a high impact on Canadians, the operations of the government, and/or its employees. The level of criticality can be determined based on a series of criticality criteria provided in Appendix D. Within the context of this guide, functions will be classified as government-wide mission-critical or department-wide mission-critical.
- Time event horizon: A date or point in time when a specific asset will experience the impact of its Year 2000 problem, which may be a date in advance of 2000.
- Year 2000 compliance: Year 2000 compliant means that the asset 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.

2. Year 2000 Taxonomy

2.1 How to Use the Year 2000 Taxonomy

The TBS Business Continuity Guide [Reference 1] provides detailed sections devoted to conducting risk identification and analysis in support of Year 2000 projects.

The main tool utilized in identifying Year 2000 project risks is the Year 2000 Taxonomy as depicted in the diagram below. The Year 2000 Taxonomy is a questionnaire used in a workshop or interview setting that highlights important aspects of a Year 2000 project life-cycle which must be addressed otherwise issues/problems may arise. The information captured as a result of the risk identification and analysis activities is to be documented and formatted as per the TBS Year 2000 Risk Information Sheet [Reference c].



Communicate = communiquer
Identify = identifier
Analyze = analyser
Plan = planifier
Track = suivre
Control = contrôler

Figure H-1 – "Conduct Risk Assessment" Activity

2.1.1 Participants to the Workshop or Interview

The TBS Year 2000 Taxonomy can be used during a 3 hour workshop or ½ - 2 hour interview with project stakeholders. These Year 2000 project stakeholders may include resources such as the Year 2000 project office personnel including the Project Manager, practitioners, Year 2000 Steering Committee members, the Year 2000 Project Director, the Year 2000 Project Sponsor, other senior executives (ADMs, DMs), business line managers (including personnel), and technical managers (including personnel responsible for applications, infrastructure, facilities, etc.).

2.1.2 Tailoring

The TBS Year 2000 Taxonomy is a comprehensive questionnaire used to support the identification of Year 2000 risks during a risk assessment (risk identification and analysis). Ideally all questions should be asked, however, the taxonomy may contain questions that are not relevant to some participants of the risk assessment, or relevant at a particular point in the Year 2000 project life-cycle.

As a guideline to help with the tailoring of the questionnaire, an indicator has been associated with each question to identify a mandatory (answer required) or tailorable question. The questionnaire can also be tailored for the type of personnel being interviewed. As a general rule, the questionnaire can be tailored as follows:

a. The questions for Section 1.1 – Year 2000 Project Life-Cycle Processes are targeted at most stakeholders;

b. The questions from Sections 1.2 to 1.5 and 2.1 – Technical/Project Management are mainly targeted at Year 2000 project office personnel and technical managers; and

c. The questions from Section 2.2 – Business/Program Management are mainly targeted at the business line managers and senior executives.

An additional suggested approach for tailoring the questions is to determine your organization's Year 2000 project stakeholders (as in section 2.1.1 above). You then create additional columns alongside the questionnaire corresponding to the stakeholders, and check-off the questions that are to be asked to a particular stakeholder (refer to the example figure below). Overlapping questions asked to various stakeholders is considered to be acceptable and will provide different viewpoints to a particular subject area.

#	Question	Y	N	DK	NA	Stakeholder A	Stakeholder B	Stakeholder C	Stakeholder D
1.1.1						✔		✔	
1.1.2						✔	✔	✔	
1.1.3							✔	✔	
1.1.4						✔	✔	✔	
1.1.5						✔		✔	✔
.								✔	✔
N						✔		✔	✔

Figure H-2 – Example of Tailoring Questions and Targeting Stakeholders

2.1.3 During the Workshop or Interview

During the Year 2000 risk assessment workshops or interviews, questions from the TBS Year 2000 Taxonomy should be asked to the participants in order to elicit discussion and determine if a risk exists in the subject area. The facilitator for the risk identification workshop/interview should also attempt to link risks to the business functions of the department.

The general steps include:

a. Ask a question;

b. Obtain the response to the question as follows:

   i) **Yes** – This is considered to be a positive response to the question indicating that there is no risk with regards to the subject area of the question;

   ii) **No** – This is considered to be a negative response to the question indicating that there may be a certain level of risk with regards to the subject area of the question. The risk including the potential negative consequence must be recorded including any contextual information;

   iii) **Do Not Know** – This is considered to be an uncertain response to the question indicating that there may be a risk with regards to the subject area of the question. Further investigation is required outside of the workshop or interview in order to determine if there is a risk; and

   iv) **Not Applicable** – This response means that there is no risk with regards to the subject area of the question. Ensure that the question and context is well understood (refer to c. below).

c. Ask the sub-questions to ensure that the context of the question is well understood;

d. As a result of asking a question, the workshop facilitator may have to pursue the risk area beyond the question. This requires expert knowledge of the Year 2000 project in order to be able to react to this situation; and

e. Capture and record the risk statement and any context information about the risk (refer to next subsection).

2.1.4 Recording Risks

The risks identified as a result of the risk identification process should be documented using the TBS Year 2000 Risk Information Sheet [Reference c] serving as the primary means for documenting and retaining information about a risk.

2.2 Year 2000 Taxonomy Questionnaire

The TBS Year 2000 Taxonomy Questionnaire is located in Addendum 1 to this appendix.

2.3 Year 2000 Taxonomy Questionnaire Data Element Definition

This table describes the data elements (column headings) in the TBS Year 2000 Taxonomy.

Table H-1: Year 2000 Taxonomy Questionnaire Data Element Definition

Field Name	Description
Tailor	This is a guideline for tailoring the TBS Year 2000 Taxonomy. The guideline will ➢ **M** means mandatory question. (This question must be asked); and ➢ **T** means a tailorable question.
Question	The first question in the column is the main question, versus sub-questions (if applicable). The main question is the means for identifying risk in a particular Year 2000 life cycle phase or management area. Sub-questions are not considered to be part of the main question, but rather help provide context for the main question.
Yes	A positive response to the question indicates that there is no risk with regards to the subject area of the question.
No	A negative response to the question indicates that there may be a certain level of risk with regards to the subject area of the question.
Do Not Know	An uncertain response to the question indicates that there may be a risk with regards to the subject area of the question.
Not Applicable	The question does not apply signifies that there is no risk with regards to the subject area of the question.
Observation	An observation is considered to be contextual information for an identified risk. Observations may also arise from discussions with regards to the sub-questions.

2.4 Guidelines and Tips

The following guidelines and tips are aimed at improving the use of the Year 2000 Taxonomy during risk assessments:

a. Risk identification workshops should include peer groups with a common interest such as Year 2000 project office personnel, practitioners, Year 2000 Steering Committee members, business line resources, and technical resources (including personnel responsible for applications, infrastructure, facilities, etc.);

b. Risk identification workshops work best with 10 participants or less;

c. Risk identification interviews are generally conducted with senior executives such as Year 2000 project director, Year 2000 Project Sponsor, and other senior executives (ADMs, DMs);

d. Once the TBS Year 2000 Taxonomy has been tailored, the goal is to ensure that all remaining questions have been answered by a Year 2000 project stakeholder;

e. A common understanding of the risk can be obtained by querying various stakeholder groups with similar questions; and

f. State risks in objective terms, making sure that there is a potential negative impact on business continuity objectives.

Addendum 1 to Appendix H
Year 2000 Taxonomy

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
	1 Year 2000 Project Life-Cycle Processes					
	1.1 Awareness/Inventory					
M	1.1.1 Is the Year 2000 problem among the top priorities of your organization? a. Has senior management issued a formal correspondence confirming the priority of the Year 2000 project?					
M	1.1.2 Is the awareness level across your organization reflective of the priority level required by Year 2000 activities?					
M	1.1.3 Is there a Year 2000 communication plan/strategy in place? a. Does it include communications to internal and external stakeholders? b. Is your organization communicating with other government departments or organizations on Year 2000 issues (may include participation to various industry Year 2000 groups)? c. Is it effective?					
M	1.1.4 Has your organization identified all its mission-critical business functions? a. Is the list complete? b. Is the list accurate? c. Has it been communicated to TBS? d. Have the mission-critical business functions been prioritized? e. Has your organization used the TBS criticality criteria? f. Has the prioritized mission critical business function list been formally approved by senior management?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	1.1.5 Has your organization assessed the potential business impact of the Year 2000 problem on its mission-critical functions? a. Was a formal assessment methodology used to determine the impact of the Year 2000 problem?					
M	1.1.6 Has your organization identified the assets supporting the business functions? *Examples of possible assets are:* • *Internal/external systems and applications* • *Commercial-off-the-shelf systems/applications* • *IT infrastructure components;* • *Embedded systems (computerized devices that are literally embedded within a larger piece of equipment or industrial product);* • *manufacturing and process control;* • *transportation and navigation equipment (airplanes, trains, marine, traffic lights, air traffic control, etc.);* • *facilities (electrical supply, lighting, heating, ventilation, elevators, locks, security, etc);* • *office systems and mobile equipment (fax, copier, video, televisions, cell phones etc.);* • *medical devices (pacemakers, monitoring systems, x-rays, etc.);* • *lab equipment;* • *Public infrastructure/utilities/telecommunications; and* • *Other branches/departments interfaces.* a. Is the list complete? b. Is the list accurate? c. Has your organization determined the nature, size, and complexity of the assets? d. Are dependencies and/or interfaces to external assets identified?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	1.1.7 Has your organization's asset inventory been prioritized? a. Was an approach used for prioritization? b. Is the prioritization approved by senior management?					
M	1.1.8 Is there a controlled repository of the asset inventory information? a. Is it available to all Year 2000 stakeholders (for read access)?					
M	1.1.9 Has the number of assets in the inventory remained unchanged since the completion of the inventory phase?					
M	1.1.10 Have owners for business functions and assets been clearly identified? a. Have their roles and accountability been clearly defined?					
	1.2 Assessment (Analysis/Design)					
M	1.2.1 Have Year 2000 compliance requirements been defined for all types of assets? a. Have they been properly communicated to Year 2000 staff and asset owners? b. Are they documented in a guide?					
M	1.2.2 Has a standard for dates been established and approved? a. Does it include interfaces? b. Is the standard documented in a guide?					
M	1.2.3 Are resources, assigned to the assessment phase, appropriately trained in assessment techniques and tools, and knowledgeable of the assets being assessed?					
M	1.2.4 Has your organization determined the number of assets which are susceptible to the Year 2000 problem?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	1.2.5 Has your organization determined the time event horizon (a date which could be before 2000) for Year 2000 failure for all assets that are susceptible to the Year 2000 problem?					
M	1.2.6 Has the magnitude/impact of the year 2000 problem been established for each asset or asset type? a. Has this information been documented in the asset inventory?					
M	1.2.7 Are the assets accurately documented? Do they include: a. Design documents? b. As built specifications? c. Test data (if applicable)? d. Location of source code (for assets such as internal applications)? e. Identification of vendor/manufacturer (for assets such as commercial-off-the-shelf systems and embedded systems)?					
M	1.2.8 Has a triage (repair, re-engineer, replace, or retire) been conducted on the assets?					
M	1.2.9 Has the triage on assets been approved by senior management?					
M	1.2.10 Have the conversion techniques and tools been identified for asset types? a. Have they been documented in a guide? b. For IT applications, has the impact of these techniques/tools on performance been evaluated?					
T	1.2.11 For assets requiring replacement, have vendors been solicited for Year 2000 compliance?					
T	1.2.12 Have issues with electronic partners (e.g. electronic output and input requirements) been identified and resolved? a. Have the decisions been recorded?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
T	1.2.13 For assets utilizing external source data (such as application software), has a data conversion strategy been identified? a. Has the impact of data conversion on performance been evaluated?					
T	1.2.14 For IT assets, will the existing IT infrastructure support the added load of Year 2000 conversion activities?					
T	1.2.15 For IT assets, have the changes to the IT production environment (HW, SW, network) been identified and costed?					
M	1.2.16 Have issues with vendor responses for Year 2000 compliance been identified and resolved? a. Have the decisions been recorded?					
M	1.2.17 Have the results from the assessment phase been used to re-evaluate/confirm the effort estimates and budget?					
T	1.2.18 Have vendors been solicited for their Year 2000 strategy with respect to their suppliers (supply chain issues)?					
M	1.2.19 Have business continuity artifacts been collected (e.g. business resumption plans, disaster recovery plans, etc.)? If yes, are they up-to-date?					
M	1.2.20 Has the ability of the organization to ensure business continuity been assessed? If yes, were deficiencies identified and resolved?					
M	1.2.21 Have relevant crisis scenarios been identified and documented?					
	1.3 Renovation (Build)					
M	1.3.1 Are resources, assigned to renovation activities, appropriately trained in renovation techniques and tools, and knowledgeable of the assets being renovated?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	1.3.2 Can your organization state the exact number of assets that have been converted (repaired or replaced) to date?					
M	1.3.3 For assets requiring replacement, have Year 2000 compliant versions of the assets been ordered? a. Is your organization aware of the lead-time for delivery? b. Is anything being done to ensure that new or upgraded third party/vendor's assets are Year 2000 compliant?					
M	1.3.4 Have issues with renovation activities been identified and resolved? a. Have the decisions been recorded?					
T	1.3.5 Has your organization planned for the development of bridges and filters to handle non-conforming data? a. Has the number of bridges and filters increased since the completion of the assessment phase?					
M	1.3.6 Is the following documentation being updated as part of renovation activities: a. System documentation? b. User documentation? c. Training documentation? d. Test cases, etc.?					
M	1.3.7 Has unit/component testing been conducted (where applicable)?					
M	1.3.8 Have issues with regards to Year 2000 compliance for suppliers and business partners been identified and resolved? a. Have the decisions been recorded?					
M	1.3.9 Are standards being adhered to?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
T	1.3.10 Have the phase out plans for assets, scheduled for retirement, been prepared? a. Have the stakeholders been notified?					
M	1.3.11 Are contingency plans, at the business function level, in place? a. Have the time thresholds been identified for initiating the contingencies?					
	1.4 Validation (Testing)					
M	1.4.1 Have the types of resources required for validation activities been identified (such as users, business/functional resources, and technical resources)?					
M	1.4.2 Are there sufficient resources for conducting testing activities?					
M	1.4.3 Does test coverage include full functional testing as opposed to only Year 2000 specific testing?					
M	1.4.4 Has test data (where applicable for assets such as application software) been developed, collected and/or converted to support the validation activities?					
M	1.4.5 Are automated test tools/equipment in use? a. Have automated test tools/equipment been verified for Year 2000 compliance?					
M	1.4.6 Do you have sufficient time allocated for the testing activities that have been planned to be conducted?					
M	1.4.7 Is problem tracking and reporting being utilized for the Year 2000 project? a. Do you track problems until their resolution? b. Do you utilize an automated tool?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	1.4.8 Has the corrective action process (the protocol for the fixing of problems encountered) during the validation phase been properly identified and documented? a. Has enough time been allocated for problem resolution in the schedule? b. Is the feedback loop to individuals renovating the assets adequate? c. Is regression testing part of this process?					
M	1.4.9 Is the Year 2000 certification of assets a formal approval process?					
	1.5 Implementation					
M	1.5.1 Is Year 2000 related client training planned for the implementation of new or modified systems?					
M	1.5.2 Are all the contingency procedures for the restoration of assets in place and ready to be activated? a. Have contingency procedures been tested? b. Have all personnel been trained?					
M	1.5.3 Have conflicts with current operations and maintenance activities been identified?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
	2 Management					
	2.1 Technical / Project Management Processes					
M	2.1.1 Is there a Project Charter for the Year 2000 Project? a. Is the project charter understood and accepted by all stakeholders? b. Has the project charter been signed by all stakeholders (including external interface organizations)?					
M	2.1.2 Is there a Project Management Plan? a. Does it include: • *Work Breakdown structure (project activities)?* • *Organization Breakdown structure?* • *Responsibility Assignment Matrix?* • *Resource estimates?* • *Detailed budget?* • *Master Schedule?* b. Is project planning being conducted according to your organization's policies, guidelines, and procedures?					
M	2.1.3 Is the Project Management plan based on an industry approved Year 2000 life cycle or approach complete with structured activities?					
M	2.1.4 Are there plans (or work packages) for Year 2000 activities at the asset level?					
M	2.1.5 Has the Year 2000 budget been fully approved until implementation? a. If required, has a TB Submission for the Year 2000 project been created and submitted?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.1.6 Is there a Year 2000 Project Management Office (PMO)? a. Is it properly staffed? b. Does the personnel have the proper expertise and experience to support the Year 2000 project?					
M	2.1.7 Has a manager been assigned the responsibility of defining and fulfilling the Year 2000 project objectives *(converting Year 2000 susceptible assets in order to maintain business continuity beyond 2000, within the estimated budget and timeframe)*? a. Is the manager empowered to deliver this project? b. Does the manager have budget and decision making authority? c. Does the manager have a clearly defined escalation path for actions required by senior authorities? d. Is the manager a senior manager in your organization?					
M	2.1.8 Is there a Year 2000 steering committee? a. Is there adequate stakeholder representation on the committee? b. Does it include representation from all Regions? c. Is the purpose of the committee clearly identified? d. Are there frequent meetings? e. Are minutes/actions written and given to the PM?					
M	2.1.9 Is cooperation among the stakeholders effective?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.1.10 Is the master schedule realistic for mission critical business functions/assets? a. Does it include all activities until implementation? b. Are the dependencies between tasks (especially between software applications) identified on the schedule? c. Is there a critical path? d. Does it include external dependencies and/or interfaces?					
M	2.1.11 Does the project have scheduled checkpoints or “gates” when it will be reviewed and where management will decide on its future, and if necessary, take appropriate corrective action?					
M	2.1.12 Is there an audit plan for the Year 2000 project?					
M	2.1.13 Is the project plan updated to reflect the results uncovered during the previous Year 2000 life-cycle phase? a. Has there been a review of the critical path?					
M	2.1.14 Are internal project reviews conducted periodically with asset category owners/conversion teams to track progress and issues?					
M	2.1.15 Does your organization track actual progress against the year 2000 planned activities (as identified on the master schedule)? a. Have you identified adequate metrics to capture? b. Are proper management systems available to adequately monitor and control project activities? c. Is this level of monitoring adequate to support decision-making and to report progress to senior management?					
M	2.1.16 Are frequent progress reports available? a. Are issues/actions identified and acted upon?					
M	2.1.17 Are the budget and schedule stable (unchanging)?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.1.18 Are your organization's budget and schedule intermediate objectives being met?					
M	2.1.19 Are there critical success factors established for the Year 2000 project? a. Have they been translated into the acceptance or Year 2000 certification process?					
M	2.1.20 Has a human resource strategy been developed and approved?					
M	2.1.21 Have the human resource requirements for each phase been allocated? a. Are the human resource requirements stable (unchanging)? b. Have the required staff skill sets been identified?					
M	2.1.22 Has your organization re-assigned resources to the Year 2000 project when requested?					
M	2.1.23 Do you have access to the right people when you need them? a. Are people fulfilling their roles and responsibilities as identified in the project charter?					
M	2.1.24 Have all the systems, tools, and facilities required for each phase been identified, committed or acquired? a. Have these systems and tools been assessed for Year 2000 compatibility?					
O	2.1.25 Are all the contracts for the resources to be procured in place (human, computing, facilities, etc.)?					
T	2.1.26 Are the contracts secured beyond Year 2000?					
M	2.1.27 Are Year 2000 warranty clauses being inserted in contracts for goods and services (where applicable)?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.1.28 Is there a documented risk management process (including tools, techniques, practices) being utilized?					
M	2.1.29 Are risk action plans being developed and implemented to manage identified risks on the Year 2000 project?					
M	2.1.30 Is project tracking and oversight being conducted? a. Is it being conducted according to your organization's policies, guidelines, and procedures? b. Is it adequate?					
T	2.1.31 Is subcontractor management being conducted? a. Is it being conducted according to your organization's policies, guidelines, and procedures? b. Is it adequate? c. Is the subcontractor's performance monitored on a regular basis?					
M	2.1.32 Is quality assurance being conducted? a. Is it being conducted according to your organization's policies, guidelines, and procedures? b. Is it adequate? c. Have critical success factors clearly been identified?					
M	2.1.33 Is configuration management performed? a. Is it being conducted according to your organization's policies, guidelines, and procedures? b. Is it adequate? c. Are changes to code, systems, and documentation controlled? d. Does it include external interfaces?					
M	2.1.34 Is there a Crisis Management organization? If yes, is the organization trained and tested with scenarios?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.1.35 Has a Crisis Operations Centre been established? Does the organization have a pre-designated spokesperson for crisis events to inform your end users (client?)?					
M	2.1.36 Is there a business continuity plan for the organization? Does it address risk management, contingency planning, crisis response and business resumption activities?					
M	2.1.37 Has a top-level executive been identified to lead the crisis management team? Is this person aware of their responsibilities?					
	2.2 Business /Program Management					
M	2.2.1 Are there any system development/upgrade projects currently in progress? a. Are these projects approved by your senior management? b. Will these projects be Year 2000 compliant? c. Will these projects require interfacing with the existing Year 2000 compliant infrastructure or other systems?					
O	2.2.2 Are there any plans to minimize non-Year 2000 initiatives until the Year 2000 problem is resolved or under control?					
M	2.2.3 Is disruption to operations and production service levels being monitored?					

Tailor	Question	Yes	No	Do Not Know	Not Appli-cable	Observations
M	2.2.4 Has the current business environment been evaluated for constraints that may impact the Year 2000 project implementation? a. Program delivery? b. Legislation? c. Political?					
M	2.2.5 Has your organization assessed its legal liabilities associated with the Year 2000 problem and potential business function failures? a. Is your Legal branch/representative involved?					
M	2.2.6 Have you discussed your Year 2000 Plan with your organization's Legal representative?					
M	2.2.7 Is your organization's Legal representative conducting a Legal Risk Assessment?					
M	2.2.8 Is there a legal action plan?					

Appendix I
Risk Information Sheet

1. Introduction

1.1 Background

The Treasury Board of Canada Secretariat (TBS) Year 2000 Project Office requires that Federal Departments and Agencies with Government-Wide Mission-Critical (GWMC) business functions identify, report and manage Year 2000 project risks.

In order to standardize the risk reporting requirements for content and format, a Year 2000 risk information sheet (RIS) is provided to document relevant information about a risk.

1.2 Purpose

The purpose of this appendix is to define and describe the TBS Year 2000 RIS to be used by Federal Departments and Agencies in reporting information regarding the Year 2000 project risks associated with the Government-Wide Mission-Critical (GWMC) and Department-Wide Mission-Critical (DWMC) business functions.

1.3 Scope

This appendix includes a description of “How to use the Year 2000 RIS”, a Year 2000 RIS template, a description of the Year 2000 RIS template data elements, and a sample Year 2000 RIS.

1.4 Relationship to Other Documents

This document relates to the following documents as identified:

a. Treasury Board of Canada Secretariat, Steering government into the next millennium: A Guide to Effective Business Continuity in Support of the Year 2000 problem, October 1998.

b. Software Engineering Institute, Continuous Risk Management Guide, Carnegie Mellon University, Pittsburgh, Pennsylvania, 1996.

The Year 2000 RIS follows the principles of the Risk Information Sheet for the Software Engineering Institute’s (SEI) *Continuous Risk Management (CRM) Guide*, Appendix A-27.

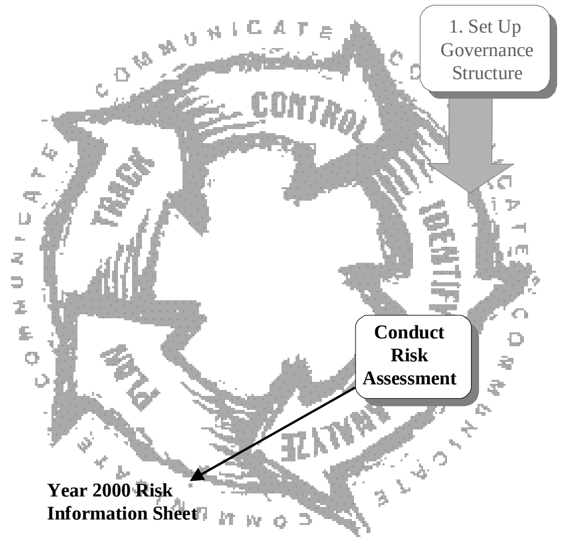
c. Treasury Board of Canada Secretariat, Year 2000 Taxonomy, October 1998. The Year 2000 RIS is the means for documenting information about risks that are identified as a result of conducting a risk assessment using the *Year 2000 Taxonomy*.

2. Year 2000 Risk Information Sheet

2.1 How to Use the Year 2000 Risk Information Sheet

The Treasury Board of Canada Secretariat Business Continuity Guide [Reference 1] provides a detailed section devoted to conducting risk assessments on Year 2000 projects. Risk assessments include the “Identify” and “Analyze” processes of the SEI CRM methodology.

The information captured as a result of the risk assessment activity is to be documented and formatted as per the Year 2000 RIS. The Year 2000 RIS serves as the primary means for documenting and managing information about a risk, and is the main deliverable for the risk assessment activity as depicted in the diagram below.



Communicate = communiquer
Identify = identifier
Analyze = analyser
Plan = planifier
Track = suivre
Control = contrôler

Figure I-1 – “Conduct Risk Assessment” Activity

The Year 2000 RIS is comprised of five sections:

a. Risk assessment information;
b. Risk management information;
c. Business information;
d. Status information; and
e. Risk action plan information.

The first four sections are mandatory risk reporting requirements by the TBS. Details of the template data elements are provided in this appendix. Section 5 of the RIS is an optional section that is provided as a guideline for the department/agency to use in developing and implementing risk management activities.

2.2 Year 2000 RIS Template

The following template constitutes the TBS Year 2000 RIS.

RISK INFORMATION SHEET
(PART 1 – TBS Required)

Department/Agency:					
1. RISK ASSESSMENT INFORMATION					
Rank:		**Risk Id:**		**Identified on:**	
Risk Statement:					
Context/background:					
Probability:					
Project Impact:					
Time frame:					
Source:					

Response:		**Escalate:**	Other	________________		□
			TBS	□	DM	□
			ADM	□	Steer.Com	□

2. RISK MANAGEMENT INFORMATION	
Assigned to:	**Action Plan Due Date:**
Risk Management Strategy Overview:	
Indicators/metrics for risk materialization:	**Means collected:**

3. BUSINESS INFORMATION				
Business Function(s):		**Criticality**	Government-Wide Department-Wide	□ □
Business Impact:				
Contingency Plan:				
Trigger:				

4. STATUS INFORMATION	
Status:	**Status date:**
Approval:	**Closing date:**

RISK INFORMATION SHEET (PART 1 – TBS Required)	
Department/Agency:	
Closing rationale:	

RISK INFORMATION SHEET (PART 2 – Risk Management Details)					
Department/Agency:					
Rank:		**Risk Id:**		**Identified on:**	
5. RISK ACTION PLAN INFORMATION					

Action Item	Responsibilit y	Date Due	Date Completed

Notes:

2.3 Year 2000 RIS Template Data Element Definition

This table describes the data elements in the TBS Year 2000 RIS.

Table I-1 – RIS Data Elements

Field Name	Description
Section 1. Risk Assessment Information	
Department/Agency	The Federal Government department or agency that is reporting risks on their Year 2000 project.
Rank	Rank or priority, in numeric format (1 through "N"), assigned to the risk. The rank should reflect the risk ranking within the department/agency at the time that the risk is reported
Risk Id	Unique identifier for the risk, which is generally a combination of a category name for the risk and a sequential numbering scheme (e.g. Management –001).
Identified on	Date when the risk was identified.
Risk Statement	Statement of the risk which is comprised of a description of the condition or circumstance causing concern or uncertainty for a potential loss or negative outcome with respect to the compliance and business continuity objectives. *[details for developing a risk statement can be found in the Reference 2 - part2, chapter 4, section 2, p.31]*
Context/background	Associated information that clarifies the risk. Context is usually gathered at the time of identification.
Probability	Likelihood of occurrence of the risk – exact value depends on the type of analysis. A suggested approach is to utilize a qualitative description as follows: ➢ **Low** (the risk will unlikely materialize, but could occur), ➢ **Medium** (the risk will likely materialize), ➢ **High** (the risk is almost certain to materialize)
Project Impact	The loss or negative outcome on the project if the risk materializes. One of the following values is required: ➢ **Low** (the impact will be minimal or negligible), ➢ **Medium** (the impact will be moderate), ➢ **High** (the impact will be critical or catastrophical)
Timeframe	Timeframe in which the risk will occur or action is needed. One of the following values is required: ➢ **Near** (30 days), ➢ **Mid** (60 days), ➢ **Far** (the time event horizon for asset failure due to the Year 2000 problem/contingency trigger). *Departments can use a timeframe that is more relevant to their environment.*

Field Name	Description
Source	The source of the risk (reason why there is a risk). One of the following values is required: ➢ **Lack of Information**, ➢ **Lack of control** (over budget, human resources, approvals/decisions etc.), ➢ **Lack of time**,
Response	The department's/agency's response to the risk. One of the following values is required: ➢ **Assume** (do nothing), ➢ **Avoid** (take actions prior to risk occurring), ➢ **Control** (take actions after risk occurs), ➢ **Transfer/Escalate** (transfer the responsibility of mitigating the risk to another party within the department/agency)
Escalate	A flag which indicates that the risk is being escalated to another organization/management level such as: ➢ **Other** - Other organizations such as National Planning Group, Emergency Preparedness Canada, etc. ➢ **TBS** - Treasury Board of Canada Secretariat ➢ **DM** - Deputy Minister ➢ **ADM** - Associate Deputy Minister ➢ **Steer. Com.** - Year 2000 Steering Committee
Section 2. Risk Management Information	
Assigned to	The person within the department/agency who is responsible for managing the risk.
Action Plan Due Date	The completion date for the activities as identified in the action plan to manage the risk.
Risk Management Strategy Overview	The selected strategy for managing the risk. This strategy is a high-level description that provides a general direction and takes into account the source and the response to the risk. Generally only risks with an "avoid" or "control" response have action plans associated with them. An "assume" response does not require risk management since the department/agency has decided to live with the consequences of the risk materializing. A transfer/escalate will require a response from the receiving party.
Indicators/metrics for risk materialization	An indicator/metric or sign that will clearly let the Year 2000 project stakeholders know that the risk is materializing and becoming an issue or problem. The indicator should be part of progress information that is collected during the "Track" step.
Means collected	The means or manner for collecting the indicators/metrics identified in the risk materialization field.

Field Name	Description
Section 3. Business Information	
Business Function(s)	The business function(s) as identified on the TBS Government-Wide Mission-Critical function list or as identified by the department/agency's Department-Wide Mission-Critical function list. Risks may apply to more than one business function.
	The mission criticality of the business function associated with the risk in question. The mission criticality is as defined by the TBS mission criticality criteria. Only one of 2 choices is available: Government-wide or Department-wide Mission-critical.
Business Impact	The impact of the risk on the continuity of the business function as opposed to the "Project Impact" defined in section 1 of the Year 2000 RIS.
Contingency Plan	This is a reference to a contingency plan. The contingency plan should contain procedures that will restore the mission-critical business function or an asset within a business function in the event that a Year 2000 problem materializes.
Trigger	The trigger for implementing a contingency plan/procedure. The trigger will generally be the "fact" or "threshold" that indicates that the risk has materialized and/or has become a problem/issue.
Section 4. Status Information	
Status	Status of the risk. The following value is required: ➢ **Open** (Risk is still valid), ➢ **Closed** (Risk is no longer valid)
Status date	The date the last status was provided or determined.
Approval	This is a signature for approval for mitigation strategies or closure by the "Assigned To" person from section 2 of the Year 2000 RIS.
Closing date	Date when the risk was closed
Closing rationale	Rationale for closure of the risk
Section 5. Risk Action Plan Information	
Action Item	This is a series of action or steps that must be executed in order to mitigate the risk. The action items must support the risk mitigation strategy.

Field Name	Description
Responsibility	The person assigned to conduct an action item. The same person may conduct all action items on the list. This person may be the same as the "Assigned To" person from section 2 of the Year 2000 RIS or this person may be someone who has been assigned to work on the actions but still must report to the "Assigned To" person.
Date Due	The date the action item is due.
Date Completed	The date the action item was completed.
Notes	An optional field for general notes. This section could identify resources required in order to implement the risk action plan actions.

2.4 Examples of a Year 2000 Risk Information Sheet

2.4.1 Example A – Organizational/project risk

The following Year 2000 RIS is to be used as an **EXAMPLE ONLY**. This risk is based on an imaginary scenario where a department X has identified a risk regarding a lack of funding for the Year 2000 project.

RISK INFORMATION SHEET (PART 1 – TBS Required)					
Department/Agency:	Department X				
1. RISK ASSESSMENT INFORMATION					
Rank:	2	**Risk Id:**	Lack of Funding	**Identified on:**	5-Jan-1998
Risk Statement:					
There is a risk that the funding for Year 2000 activities beyond March 1998 will not be approved in time to allow the timely progression of Year 2000 related activities. The impact of this risk is that the remaining Year 2000 activities will not be conducted, thus affecting the Year 2000 project schedule.					
Context/background:					
The Treasury Board submission for funding is currently being prepared and is planned to be delivered on March 10, 1998. No Year 2000 susceptible assets have been completely converted as of 5-Jan-1998.					
Probability:	High				
Project Impact:	High				
Time frame:	Near				
Source:	Lack of control				
Response:	Avoid	**Escalate:**	Other	________________	☐
			TBS ☐	DM	☐

RISK INFORMATION SHEET
(PART 1 – TBS Required)

Department/Agency:	Department X		
			ADM □ Steer.Com ■

2. RISK MANAGEMENT INFORMATION

Assigned to:	**Action Plan Due Date:**
Mr. Y	20-Mar-1998
Risk Management Strategy Overview:	
The risk management strategy is aimed at obtaining control over funding.	
Indicators/metrics for risk materialization:	**Means collected:**
1. Schedule slippage 2. An inability to hire subcontractors	1. Master schedule/progress reports 2. Non-approval for procurement requests for hiring subcontractors

3. BUSINESS INFORMATION

Business Function(s):	All functions that have dependencies on Year 2000 susceptible assets	**Criticality**	Government-Wide ■ Department-Wide ■
Business Impact:	Year 2000 failures in the Year 2000 susceptible assets will halt operations in the following government-wide and department-wide mission-critical functions: 1. Provide service X (GWMC) 2. Pay employees (DWMC)		
Contingency Plan:	Department X contingency plan: 1. Restore "Provide service X" function - Contingency procedure 2.3.1-003 2. Restore "Pay employees" function - Contingency procedure 4.3.1-001		
Trigger:	1. If Year 2000 susceptible assets for the "Provide service X" function are not certified Year 2000 compliant by January 1, 1999, then the contingency will be implemented. 2. If Year 2000 conversion for Year 2000 susceptible assets for the "Pay employees" function is not certified Year 2000 compliant by December 15, 1999, then the contingency will be implemented.		

4. STATUS INFORMATION

Status:	**Status date:**
Open	21-Jan-1998
Approval:	**Closing date:**
Signature of "Mr. Y"	
Closing rationale:	

RISK INFORMATION SHEET (PART 2 – Risk Management Details)					
Department/Agency:	Department X				
Rank:	2	**Risk Id:**	Lack of Funding	**Identified on:**	5-Jan-1998
5. RISK ACTION PLAN INFORMATION					

Action Item	Responsibility	Date Due	Date Completed
1. Complete the Treasury Board submission for extra funding	Mr. Y	5-Feb-1998	
2. Have the Treasury Board submission signed by the senior executives and delivered to Treasury Board	Mr. Y	20-Feb-1998	
3. Obtain Treasury Board approval	Mr. Y	20-Mar-1998	

Notes:

It was decided to dedicate Mr. A and Mr. B in order to deliver the Treasury Board submission by 20-Feb-1998 instead of the planned 10-Mar-1998.

2.4.2 Example B – Technical risk

The following Year 2000 RIS is to be used as an **EXAMPLE ONLY**. This risk is based on an imaginary scenario where a department X has identified a risk regarding an inability to obtain a Year 2000 compliant version of "Equipment A".

RISK INFORMATION SHEET (PART 1 – TBS Required)					
Department/Agency:	Department X				
1. RISK ASSESSMENT INFORMATION					
Rank:	3	**Risk Id:**	Non-Year 2000 compliant Equipment A	**Identified on:**	12-Apr-1998
Risk Statement:					
There is a risk that the "Equipment A" as provided by vendor A will be discontinued since the vendor cannot provide details nor plans for Year 2000 compliance. The impact of this risk is that the existing "Equipment A" will not be certified as Year 2000 compliant.					
Context/background:					
"Equipment A" was discovered to be Year 2000 susceptible during the assessment phase of the Year 2000 project. The vendor A has not responded to our letter requesting a statement of Year 2000 compliance for a future version of "Equipment A".					

RISK INFORMATION SHEET
(PART 1 - TBS Required)

Department/Agency	Department X		
Probability:	High		
Project Impact:	High		
Time frame:	Mid		
Source:	Lack of information		
Response:	Avoid	**Escalate:**	Other ________________ □ TBS □ DM □ ADM □ Steer.Com □

2. RISK MANAGEMENT INFORMATION

Assigned to:	**Action Plan Due Date:**
Mr. Z	

Risk Management Strategy Overview:

The risk management strategy is aimed at obtaining better information regarding the ability of vendor A to provide a Year 2000 compliant version of "Equipment A".

Indicators/metrics for risk materialization:	**Means collected:**
1. Schedule slippage for the Year 2000 conversion of "Equipment A".	1. Master schedule/progress reports

3. BUSINESS INFORMATION

Business Function(s):	"Provide service C"	**Criticality**	Government-Wide □ Department-Wide ■
Business Impact:	A Year 2000 failure for "Equipment A" will degrade the "Provide service C" function to 25% capacity.		
Contingency Plan:	Department X contingency plan: 1. Restore "Provide service C" function - Contingency procedure 10.2.5-002		
Trigger:	1. A Year 2000 compliant version of "Equipment A" is not obtained by		

4. STATUS INFORMATION

Status:	**Status date:**
Open	12-Apr-1998
Approval:	**Closing date:**
Signature of "Mr. Z"	

Closing rationale:

RISK INFORMATION SHEET
PART 2 – Risk Management Details

Department/Agency:	Department X				
Rank:	3	**Risk Id:**	Non-Year 2000 compliant Equipment A	**Identified on:**	12-Apr-1998

5. RISK ACTION PLAN INFORMATION

Action Item	**Responsibilit y**	**Date Due**	**Date Completed**
1. Attempt a second contact with vendor A	Mr. Z	10-May-1998	
2. Conduct an options analysis for a replacement equipment or substitute for "Equipment A"	Mr. Z	1-Jun-1998	
3. Select replacement equipment or substitute for "Equipment A"	Mr. Z	1-Jul-1998	
4. Integrate the replacement equipment or substitute for "Equipment A"	Mr. Z	2-Oct-1998	
5. Test the replacement equipment or substitute for "Equipment A" for the Year 2000 problem	Mr. Z	10-Jan-1999	
6. Certify/validate the replacement equipment or substitute for "Equipment A" as being Year 2000 compliant	Mr. Z	3-Feb-1999	

Notes:

None.

RISK INFORMATION SHEET
(PART 1 – TBS Required)

Department/Agency:	Department X

1. RISK ASSESSMENT INFORMATION

Rank:	4	**Risk Id:**	Inability to pay benefits	**Identified on:**	8-Oct-1998

Risk Statement:

There is a risk that benefits will not be paid to eligible beneficiaries beyond January 2000.

The impact of this risk is that the economic well being of thousands of Canadians may be impacted.

Context/background:

Department X is paying benefits to over 1Million Canadians in support of Program "Y". These benefits represent the main source of income to many of these beneficiaries and are essential to these individuals.

Department X depends on several business partners to pay these benefits and has currently no control over their progress in addressing the Year 2000 problem.

Probability:	Medium
Project Impact:	High
Time frame:	Near
Source:	Lack of control

Response:	Avoid	**Escalate:**	Other	________________		□
			TBS	□	DM	■
			ADM	□	Steer.Com	□

2. RISK MANAGEMENT INFORMATION

Assigned to:	**Action Plan Due Date:**
Mr. Y	15-Nov-1998

Risk Management Strategy Overview:

The risk management strategy is aimed at obtaining control over some key business partners by formalizing their engagement to pay benefits through special legal agreements.

Indicators/metrics for risk materialization:	**Means collected:**
1. Variances in partner's plans	1. progress reports
2. Missed payments complaints from beneficiaries	2. complaint department

3. BUSINESS INFORMATION

Business Function(s):	Pay benefits	**Criticality**	Government-Wide	■
			Department-Wide	□
Business Impact:	Inability to pay benefits			

RISK INFORMATION SHEET (PART 1 – TBS Required)		
Department/Agency:	Department X	
Contingency Plan:	Manually produce cheques for beneficiaries and have them delivered through special courier service.	
Trigger:	1. Clear indication that some partners will not be ready. 2. Complaints from beneficiaries	
4. STATUS INFORMATION		
Status:		**Status date:**
Open		14-Oct-1998
Approval:		**Closing date:**
Signature of "Mr. Y"		
Closing rationale:		

Appendix J
Sample Risk List

The following sample risk list contains the following information:

a. Risk Id;
b. Risk statement; and
c. Context/background.

The definitions for these attributes are located in Appendix I – Risk Information Sheet.

Table J-1 – Sample Risk List

Risk Id	Risk Statement	Context
Contingency Planning	There is a risk that contingency plans may not be created/updated for certain Branches since this was an activity that seemed to have less priority over other operational and Year 2000 activities.	A Year 2000 contingency plan in the context of this risk is "a plan which will identify how a particular business function will be performed should a system fail due to the Year 2000 problem".
	Lack of contingency planning may result in an inability to resume certain business functions which may have social, legal and political implications;	There were discussions of disaster recovery plans and business resumption plans during the interview sessions and during the risk assessment, but very little information was provided regarding Year 2000 contingency plans.
Human Resource Planning	There is a risk that "Dept. X" may not be able to assemble all the resources needed to support its Year 2000 conversion as evidenced by resource losses to the private industry and the current significant reliance on industry to fulfill its current role.	As of July 1997, the following actions had been performed: • The Year 2000 Project Office has develop and issued a RFP for Year 2000 work;

Risk Id	Risk Statement	Context
	The impact related to this risk is schedule delays, and the possibility of not completing all of the planned Year 2000 conversions;	• The Year 2000 Project Office has initiated the development of an alternative procurement strategy for resource requirements which cannot yet be identified (business, infrastructure, Year 2000 Project Office types of resources);
		• The Year 2000 Project Office has initiated the development of a Human Resource strategy/plan;
Operational Activities	Operational activities may focus priorities away from the Year 2000 problem and place additional demands for similar resources. The potential for the outsourcing option also adds more uncertainty and complexity in an environment that is already complex. The impact related to this risk is an increase in resource requirements and the potential for some Year 2000 conversions to not be ready on time.	Many development projects are being conducted in parallel such as project "X", "Y", and "Z".

Appendix K
Sample Business Continuity Artifacts

Sample business continuity artifacts include:

- Business resumption plans;
- Disaster recovery plans;
- Standard operating procedures (may contain some business continuity elements);
- Operations manuals (may contain some business continuity elements);
- Inventories (including tape libraries);
- Lessons learned documents from previous crises;
- Personnel list (including up-to-date phone list);
- Facilities list (including addresses, phone numbers, contact, etc.);
- Departmental Information;
- Emergency Service Agreements;
- Key Client/Customer List;
- BRP Equipment Supplies List;
- Information Technology Application List;
- Information Technology Equipment List;
- Office Equipment List;
- Other Equipment List;
- Key Vendor/Supplier List;
- Primary/Secondary Team Contact Sheets;
- Offsite Storage/Vital Records Log; and
- Incident Log.

Appendix L
"Analyze" Detailed Procedures

Process Overview

Risk analysis follows the identification step and is aimed at obtaining risk information that can be used for decision-making on the Year 2000 Project. The following table provides the details to the analyze step. Detailed procedures for analyzing and determining the contingency planning requirements are provided in Appendix N.

Table L-1 – Analysis Steps

Risk Analysis Steps	Description	Responsibility
1. Conduct a Risk Analysis Workshop	Identify a subset of stakeholders from the various risk identification workshops in order to conduct a risk analysis workshop intended to analyze each risk.	Year 2000 Project Manager
2. Conduct Tri-level Attribute Evaluations for each Risk.	During the risk analysis workshop, determine the following qualitative attributes for each risk: Probability: High, Medium, or Low; Impact: High, Medium, or Low; and Timeframe: Near, Mid, or Far; *(Refer to risk information sheet for details – Appendix I)*	Year 2000 Project Manager
3. Determine the Source of the Risk.	During the risk analysis workshop, determine the source for each risk as follows: • Lack of information: This source of risk implies that the project/department has a lack of information regarding the likelihood of the event (risk) and/or its consequence. (e.g. risks related to the use of new technologies are often the result of a lack of information about the potential/performance of these technologies); • Lack of control: • This source of risk implies that the project/department has a lack of control over the likelihood of the event (risk) and/or its consequence (e.g. lack of control over resources, budget, authority etc.); or	Year 2000 Project Manager

Risk Analysis Steps	Description	Responsibility
	• Lack of time: This source of risk implies that the project/department does/will not have the time to identify the risks associated with the project or a given course of action. It can also imply that the project will not have the time to assess the probability of occurrence or the impact of a given risk.	
4. Determine the Response to the Risk.	During the risk analysis workshop, determine the response to each risk as follows:	Year 2000 Project Manager
	• Assume: Let the risk occur, do nothing about it, and accept the consequences; • Avoid: Develop and implement mitigation strategies/risk action plans prior to the risk occurring;	
	• Control: Develop risk mitigation strategies/risk action plans to be implemented after the risk occurs; and	
	• Transfer: Transfer the responsibility of mitigating the risk to a third party, however, the department still has to track and control this risk since there is no guarantee that the transferee will be successful in mitigating the risk. • Escalate Escalate the responsibility of the risk to another organization/management level such as: ➢ **Other** - Another organization/party who can help manage the risk ➢ **TBS** - Treasury Board of Canada Secretariat ➢ **DM -** Deputy Minister ➢ **ADM -** Associate Deputy Minister **Steer. Com.** - Year 2000 Steering Committee	

Risk Analysis Steps	Description	Responsibility
5. Determine the Risk Rank.	During the risk analysis workshop, conduct a risk ranking activity using one of the following three techniques: 1. Comparative risk ranking (refer to the CRM Guidebook) – a method for comparing each risk against each other and determining which risk is more significant; 2. Multivoting (refer to the CRM Guidebook) - an average of all individual voting/ranking; or 3. Top N (refer to the CRM Guidebook) - the top risks which are significant, with a probability and impact of “medium” or “high” As a guideline, risks with “low” probability and “low” impact should be discarded from the prioritization exercise. In order to conduct efficient risk management, it is important to deal with the risks that have medium to high probability and impact.	Year 2000 Project Stakeholder (Year 2000 PO resources plus others from within the department)
6. Approve the new Risks	The Year 2000 Project Manager approves the risks identified on the final risk list.	Year 2000 Project Manager
7. Develop the Risk Information Sheets.	Once the risks are approved, document the risks using a Risk Information Sheet (refer to Appendix I). Each Risk Information Sheet will form the basis for managing each risk identified.	Year 2000 Project Manager

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.

Appendix M
Sample Risk Assessment Report – Table of Contents

A risk assessment report should provide the following sections following the content requirements of the guide sections 3 (Identify) and 4 (Analyze).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. INTRODUCTION
    1.1 Background
    1.2 Purpose
    1.3 Scope
    1.4 Objectives
    1.5 References

2. METHODOLOGY

3. RISK ASSESSMENT RESULTS
    3.1 Risk Assessment Summary
    3.2 Observations
    3.3 Problems
    3.4 Detailed Risk Assessment
    3.5 Sources Types
        3.5.1 Sources of Risks
        3.5.2 Source Analysis Results
    3.6 Responses Types
        3.6.1 Responses to Risks
        3.6.2 Response Analysis Results

4. RISK MANAGEMENT STRATEGIES
    4.1 Risks to be Assumed
    4.2 Avoidance Strategies
    4.3 Control Strategies
    4.4 Transfer Strategies

5. CONCLUDING REMARKS
    5.1 Next Step
    5.2 Conclusion

APPENDICES
Appendix A – Risk Assessment Participants
Appendix B – Comparative Risk Ranking Results
Appendix C – Total Risk Estimation (TRE) Matrix

Appendix N
Business Continuity Requirements Definition
Detailed Procedures

Process Overview

An essential element of business continuity is the determination of when and where contingency plans should be developed and implemented. The following table provides steps to assist departments in making this determination. This procedure should be applied during the "analyze" step.

Table N-1 – Contingency Planning Requirements Definition Detailed Procedure

Steps	Description	Responsibility
1. Conduct a business impact analysis	Using the prioritized **mission-critical** business function list and associated asset mappings from the "Identify" step, as well as the Risk Information Sheets from the "Analyze" step, conduct a business impact analysis. Input may also be required from the Year 2000 Project/Program Office with respect to progress on assets being made Year 2000 compliant.	Function Owner
	For <u>each</u> mission-critical business function: a. Has a risk been associated with the mission critical function or any of its mapped assets?	
	• **YES** – Then a contingency is required for the business function. Go to Step #2 to determine the contingency requirement details for the business function. • **NO** – Go to the next question Step #1-b).	
	b. In addition to any risk assessment information, are any assets that are mapped to the business function vulnerable to a Year 2000 failure?	
	• **YES** – Then more analysis is required to determine whether a contingency is required for the business function. Go to Step #1-c). • **NO** – Then no contingencies are required for the business function/asset. Document this decision and have senior management approve it.	
	c. Is the asset(s) that is considered to be vulnerable to a Year 2000 failure required (or considered a significant contributor) in delivering the business function's services/products (or delivering a minimal acceptable level of service)?	

Steps	Description	Responsibility
	• **YES** – Then a contingency is required for the business function. Go to Step #2 to determine the contingency requirement details for the business function. • **NO** – Then no contingencies are required for the business function/asset. Document this decision and have senior management approve it. *Note: Departments need to instruct their personnel on the department's response to risk (i.e. totally risk averse, willing to accept some risks, etc.) in order to guide this exercise.*	
2. Develop a draft/high level contingency for the entire business function?	For each business function associated with a known risk (Step 1-a) or has vulnerable assets from Step 1-c), develop a contingency plan to address a potential failure (can be total or limited to one or a combination of assets). Factors to consider at this stage are: 1. Level of functionality required to replace the minimum acceptable service level. 2. The minimum acceptable level of functionality to replace the functionality from the asset. 3. Are all assets in the category required or is a subset acceptable to maintain the minimum service levels required by the business function? 4. What type of contingency will be employed: manual; semi-automated; or automated replacement. 5. Implementation schedule: – When should the contingency be implemented (acquired, tested, trained, maintained, deployed)? – Who will do perform these activities? – How long is the contingency required for? – What will trigger the contingency implementation? – Cost of the contingency implementation	Function Owner
3. Monitor Progress Report	For <u>each</u> mission-critical business function and mapped asset: a. Is there is a concern with the Year 2000 readiness based on variance in schedule, successive slippages, etc.?	Function Owner

Steps	Description	Responsibility
	• **YES** – Verify the contingency plan to ensure that there exists a contingency for the asset and for the business function. If there are no contingencies, develop a contingency as per Step #2, then go to Step 3b). • **NO** – Continue to monitor the environment and go to the next question Step #4 or #5. b. Is the concern with the progress at a threshold where the contingency should be triggered? • **YES** – Implement the contingency. • **NO** – Continue to monitor the environment and go to the next question Step #4 or #5.	
4. Monitor Continuous Risk Management Activities	For <u>each</u> mission-critical business function and mapped asset: a. Are any of the identified risks materializing based on the indicators on the risk information sheets? • **YES** – Implement the contingency associated with the risk. • **NO** – Continue to monitor the environment and go to the next question Step #5 or #3. b. Have new risks been identified? • **YES** – Verify the contingency plan to determine if there exists a contingency for the asset and for the business function. If there are no contingencies, develop a contingency as per Step #2, then go to Step 3-b). • **NO** – Continue to monitor the environment and go to the next question Step #5 or #3.	Function Owner
5. Review the Verification and Validation reports (including audit reports)	For <u>each</u> mission-critical business function and mapped asset: a. Is there is a concern with the Year 2000 readiness for an asset or function based on the verification and validation (or audit) report.? • **YES** – Verify the contingency plan to ensure that there exists a contingency for the asset and for the business function. If there are no contingencies, develop a contingency as per Step #2, then go to Step 5-b). • **NO** – Continue to monitor the environment and go to the next question Step #3 or #4. b. Is the concern with the progress at a threshold where the contingency should be triggered? • **YES** – Implement the contingency.	Function Owner

Steps	Description	Responsibility
	• **NO** – Continue to monitor the environment and go to the next question Step #3 or #4.	

Appendix O
"Plan" Detailed Procedures

Process Overview

The "plan" step is divided into separate but related types of planning documents: Risk Action Plans, Contingency Plans, and Business Continuity Preparedness Documents. The following table provides steps to develop risk action plans for the identified risks. Sample Tables of Contents are provided for the other plans.

Table O-1 – Detailed Risk Planning Steps

Risk Planning Steps	Description	Responsibility
1. Conduct a Risk Planning Workshop.	Identify key stakeholders from the Year 2000 Project in order to conduct a workshop intended to develop risk action plans for mitigating the identified risks.	Year 2000 Project Manager
2. Select Risks	*Answer "Who's risk is it?"* Review the risks identified in Risk Information Sheets (RIS) to determine their validity and to determine whether the Year 2000 PO is responsible for managing each risk. Using the Responsibility Decision flowchart (CRM Guidebook, Chapter 6, Part 2), for each risk, determine: a. Does the Year 2000 PO have the responsibility to deal with this risk? • **YES** – The Year 2000 PO will <u>Keep</u> the responsibility for this risk. Go to the next step (#3) to determine the <u>Approach</u> for dealing with the risk; • **NO** – Go to the next question step #1 - b); b. Does the functional organization have the responsibility to deal with this risk? • **YES** – Then the Year 2000 PO must <u>Delegate</u> the responsibility to the appropriate organization. Determine who is best suited to deal with the risk and then have them follow similar activities as in step #3 (determine the approach for dealing with the risk), or facilitate the process for them. The Year 2000 PO must still track the activities for this risk since it is still a risk which can have a negative impact on the Year 2000 Project;	Year 2000 Project Manager

Risk Planning Steps	Description	Responsibility
	- **NO** – Transfer the responsibility to another organization (e.g. Treasury Board) and have them follow similar activities as in step #3 (determine the approach for dealing with the risk), or facilitate the process for them. The Year 2000 PO must still track activities for this risk since it is still a risk which can have a negative impact on the Year 2000 Project.	
1. Analyze the Risks and Decide an Approach for Managing the Risks.	*Answer "What can be done about it?"* For each risk that the Year 2000 PO is responsible for (or other organization as in step #1 - b) determine whether the risk is well understood, then determine the appropriate approach for managing the risk. Using the Approach Decision flowchart (CRM Guidebook, Chapter 6, Part 2), for each risk, determine:	Year 2000 Project Manager
	a. Does the Year 2000 PO understand the risk and is the risk clearly documented in the Risk Information Sheet?	
	- **YES** – Go to the next question step #3 - b);	
	- **NO** – Conduct more research on the risk and go back to step #2 (Select risk);	
	b. Can the Year 2000 PO accept this risk without doing anything to manage or control its probability and impact (this is validating the "response" on the Risk Information Sheet)?:	
	- **YES** – No further action is required. The Year 2000 Project will Accept (or assume) any impact associated with the materialization of the risk;	
	- **NO** – Go to the next question step #3 - c);	
	c. Can the Year 2000 PO do anything with regards to this risk? Does the Year 2000 PO need to act on this risk?	
	- **YES** – Then the Year 2000 PO needs to develop Mitigation (or avoidance) strategies to be implemented before the risk materializes in order to minimize or completely avoid the probability of the risk materializing as well as minimizing its impact. Go to the next step # 4 (Generate Action Plans).	

Risk Planning Steps	Description	Responsibility
	• **NO** – Then the Year 2000 PO needs to develop Watch (or Control) strategies for managing the risk when it materializes in order to minimize the impact. Go to the next step # 4 (Generate Action Plans).	
1. Generate Action Plans	*Answer “How much and what should be done?“* For each risk that the Year 2000 PO is responsible for, and for which a “Mitigation (avoid)” or “Watch (control)” approach for managing the risk is required (resulting from step 3-c), develop various strategies to deal with the risks. This can be accomplished using a brainstorming technique. Once various alternative strategies have been clearly identified, choose the best strategy (or combination thereof) which minimizes the probability of occurrence as well as minimizes the negative impact of the risk. The selected strategy must then be elaborated by developing a risk action plan for each risk. The risk action plan is a series of action items that will direct a Year 2000 PO or departmental resource in implementing the mitigation strategy. The risk action plan is to be attached to the Risk Information Sheet.	Year 2000 Project Manager
2. Assign Year 2000 PO Risk Owner	For each risk that requires a risk action plan (those for the Year 2000 PO as well as those delegated to the department or transferred to another organization such as TBS), assign a risk owner. This person will be responsible for tracking and reporting status on each risk and associated activities (such as the development of risk action plans).	Year 2000 Project Manager
3. Ensure Risk Action Plans are Developed	For each risk that was delegated to the department or transferred to another organization, the Year 2000 PO must ensure that risk action plans are being developed for risks requiring avoidance or control. The Year 2000 PO must still track activities for this risk since it is still a risk which can have negative impacts on the Year 2000 Project.	Risk Owners

Risk Planning Steps	Description	Responsibility
4. Implement Action Plans	For each risk action plan that was developed and for which there was a risk mitigation (or avoidance) strategy required, each risk owner responsible for a risk must implement the risk action items on the Risk Information Sheet by the target implementation date. The implementation activities will be tracked and monitored for problems with the implementation.	Risk Owners

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.

Appendix P
Sample Contingency Plan – Table of Contents

A contingency plan should provide the following sections following the content requirements of the guide sections 5 (Develop Risk Action and Contingency Plans).

EXECUTIVE SUMMARY

1. INTRODUCTION
    - 1.1 Background
    - 1.2 Purpose
    - 1.3 Scope
    - 1.4 Audience
    - 1.5 Relationship to Other Plans/Reports

2. ORGANIZATION
    - 2.1 Governance Structure
    - 2.2 Key Year 2000 Contingency Planning Stakeholders

3. EXPOSURE ANALYSIS RESULTS
    - 3.1 Contingency Capability Assessment
    - 3.2 Business Function Priority
    - 3.3 Risk Assessment
    - 3.4 Contingency Requirements

4. CONTINGENCY PLANNINGACTIVITY OVERVIEW
    - 4.1 Perform Continuous Risk Management
    - 4.2 Define Crisis Scenarios
    - 4.3 Develop Contingency Plan
    - 4.4 Respond to crises
    - 4.5 Resume operations

5. CONTINGENCY PLAN TRAINING
    - 5.1 Objectives
    - 5.2 Requirements
    - 5.3 Activities

6. CONTINGENCY PLAN TESTING
    - 6.1 Objectives
    - 6.2 Requirements
    - 6.3 Activities

7. CONTINGENCY PLAN MAINTENANCE
    - 7.1 Objectives
    - 7.2 Requirements
    - 7.3 Activities

APPENDICES

Appendix A – Contingency Procedures For Mission Critical Functions

Contingency Plan Information Sheet
(PART 1 – TBS Required)

Department/Agency:

1. CONTINGENCY PLAN IDENTIFICATION

Procedure Name: **Procedure Id:**	**Business Function Impacted (Consequence):** **Business Function Id:**
System / Asset Failure Description *(Range from individual to complete asset failure)***:**	**Trigger 1:** **Trigger 2:**

Maximum Acceptable Degradation Level:

Maximum Acceptable Delay Before Resumption:

Mission Criticality: **Government-wide** □ **Department-wide** □ **Other** □	**Reviews:** **Legal:** □ **Deputy Minister's Office:** □
Functional Authority *(name)***:** **Telephone Number:**	**Asset Responsibility** *(name)***:** **Telephone Number:**

2. CONTINGENCY PLANS

Contingency Procures: *(Contingency procedure owners can attach a more detailed description of the procedure***)**

- **consists of mitigation measures**

Key Logistical Issues: *(Location of key contingency procedure tools, guides, supplies and/or resources)*

Crisis Response Procedures: (Extraordinary measures only taken under crisis)

Contingency Plan Information Sheet
(PART 1 – TBS Required)

Department/Agency:

Business Resumption Procedures: (Actions required to restore normal state of operations)

3. CONTINGENCY PLAN LIFE CYCLE:

Training Frequency:	**Test Frequency:**	**Maintenance Frequency:**
Date Last Training:	**Date Last Tested:**	**Date Last Maintained:**
Sign-off:	**Sign-off:**	**Sign-off:**

Status (Draft or Final) and Version:

Approval:

Dated:	**File Location:**

Appendix Q
Sample Crisis Scenario Definition
Detailed Procedures

This procedure supports the performance of the activity defined in Section 4.2 of the contingency plan.

Table Q-1 – Detailed Crisis Scenario Definition Steps

Step	Description	Components
Step 1	**Identify Vulnerabilities (Hazard Identification / Risk Assessment)**	• See Appendix M – Section 3.4
Step 2	**Prepare Risk List Based on Priorities and High consequence Events**	• See Appendix M – Section 4.4
Step 3	**Assess Capabilities**	• See Appendix H – Addendum 1
Step 4	**Identify Objectives of Prevention Preparedness Response (PPR) Program**	• See Appendix D
Step 5	**Prepare Crisis Response Plan (as part of PPR Program)**	• See Appendix R
Step 6	**Design / Develop Scenarios**	*Prior to undertaking the Scenario:* • Establish Scenario Situation, or Scenario Exercise based on Risk List ; • Establish Scenario Primary Objectives; • Establish Scenario Secondary Objectives; • Establish an expected Event Occurrence Summary Sheet; • Prepare Checklists; and • Prepare Observation Sheets. **Tabletop Scenarios (estimated time 4-6 weeks)** - Select a Co-ordinator; - Select Work Team for Tabletop Design Preparation; - Determine Objectives and Issues; - Determine Scope and Extent of Play; - Determine Focus and Format; - Determine Means of Assessment (typically qualitative); - Establish Schedule; and - Determine resource requirements (boardroom …).

Step	Description	Components
		Scenario Exercises (estimated time 6 - 22 weeks) - Select a Co-ordinator; and - Select Work Team for Scenario Design Preparation.
		Determine Objectives and Issues - Determine Scope and Extent of Play; - Determine Focus and Format; - Determine Means of Assessment (typically qualitative); - Establish Schedule for Scenario Exercise; and - Determine resource requirements.

Appendix R
Sample Crisis Response Plan – Table of Contents

This document elaborates further section 4.4 of the Contingency Plan.

EXECUTIVE SUMMARY

1. CRISIS RESPONSE PLAN – MANDATE
   1.1 Establish objectives for Responding to a Crisis
   1.2 Ensure management support
   1.3 Establish Mandate
   1.4 Introduction to Plan
   1.5 Acknowledgment / Sign-off sheet

2. CRISIS RESPONSE PLAN – RISK ASSESSMENT / CREDIBLE SCENARIO LIST
   2.1 Risk Identification
   2.2 Target Levels of Safety
   2.3 Risk Assessment
   2.4 Risk Mitigation / Risk Controls

3. CRISIS RESPONSE PLAN – CRISIS RESPONSE ORGANIZATION
   3.1 Executive Level Organization
   3.2 Emergency Response Team Organization
   3.3 Integration of different areas (business resumption, response teams, public information ...)
   3.4 Crisis Team contact sheet
   3.5 Crisis Team Organization – Crisis Team Leader,
   3.6 Team Contact Sheet
   3.7 Crisis Centre: Location, Map of Resources, and Supplies

4. CRISIS RESPONSE PLAN – CRISIS RESPONSE PLAN ACTION STEPS
   4.1 Crisis Thresholds and Alert Responsibilities
   4.2 Assessment / Planning Activities
   4.3 Action

5. CRISIS RESPONSE PLAN – POST-CRISIS EVALUATION
   5.1 Follow-up
   5.2 Post-Mortem
   5.3 Reporting Requirements

6. CRISIS RESPONSE PLAN COMMUNICATIONS PLAN
   6.1 Primary Contact Lists
   6.2 Secondary Contact Lists
   6.3 Media Relations

7. CRISIS RESPONSE PLAN – LEGAL / FINANCIAL CONSIDERATIONS

8. CRISIS RESPONSE PLAN – TRAINING PLAN
   8.1 Evaluation
   8.2 Methodology
   8.3 Quality Assurance Program
   8.4 Scenario Exercises
   8.5 Scenario Drills

Appendix S
Sample Business Resumption Plan – Table of Contents

This document elaborates further section 4.5 of the Contingency Plan.

TABLE OF CONTENTS

Appendix M – Offsite Storage / Vital Records Log
Appendix N – Incident Log
Appendix O – Critical Inventory List (based on Scenarios)

Appendix T
"Track" Detailed Procedures

Process Overview

Tracking should take place upon initiating the plans. The following table provides steps to track risks, and progress information.

Table T-1 – Detailed Tracking Steps

Tracking Steps	Description	Responsibility
1. Collect risk and progress information	Each risk owner responsible for a risk, must collect risk information according to the indicators identified on the Risk Information Sheet. This is to be accomplished for all risks that require avoidance or control as indicated on the Risk information Sheet. Progress information should also be collected through progress reports from the Project Office.	Risk Owners
2. Analyze risk information.	The risk and progress information obtained from step #1 is to be analyzed with respect to any thresholds established for contingency plans. New information could be compared to previous information and then a determination made as to whether the risk is materializing or progress is lacking compared to the plans.	Risk Owners

Tracking Steps	Description	Responsibility
3. Collect plan implementation status	The Year 2000 project manager must query the plan and risk owners to determine if their respective plans are being implemented and are adhering to the action plan due dates.	Year 2000 Project Manager
4. Prepare/update the risk status report.	Using the information from step #2 (on the Risk Information Sheets) and step #3, prepare or update the risk status report (i.e. exposure to business interruptions). The report should provide simple, concise and accurate status on the risks and the plans for use at the Year 2000 PO project management and Year 2000 Steering Committee meetings.	Year 2000 Project Manager
5. Report information.	The status and dispositions of risks and issues are to be discussed at the Year 2000 project management meeting and/or the Year 2000 Steering Committee meeting.	Year 2000 Project Manager and Risk Owners

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.

Appendix U
"Control" Detailed Procedures

Process Overview

Risk control takes place upon identifying variances to the risk level and plans established as part of the "Plan" step. The following table provides procedures to perform the "Control" step.

Table U-1 – Detailed Control Procedure

Control Steps	Description	Responsibility
1. Analyze status reports	The Year 2000 Project Manager, risk owner, and plan owners are to analyze the status reports provided through the "Track" activity in order to determine trends, deviations, or anomalies – this can be conducted using "cause-and-effect" analysis. The goal of this step is to clearly understand the status of each risk and plan in order to determine if further actions are required.	Year 2000 Project Manager
2. Decide on further actions.	Using the knowledge gained from the analysis step, the Project Manager must decide one of the following next steps: • Continue tracking and executing the current plan - if risk is NOT materializing; • Re-plan and make updates to the Risk Information Sheet/Plan - as required to develop more effective risk mitigation; • Invoke the contingency identified on the Risk Information Sheet or invoke the escalation process - if a risk is materializing or has an increased likelihood of materializing; or • Close the risk/Stop work - if the risk has disappeared or work is completed to the satisfaction of the Project Manager. • At any time where issues cannot be resolved then escalation to the governance structure is required.	Year 2000 Project Manager

Control Steps	Description	Responsibility
1. Execute the next step.	Implement the “control” decision from step #2 above.	Year 2000 Project Manger or other Risk Owner

Note: The responsibility currently assigned to the Year 2000 Project Manager can be delegated to other members of the organization including audit.