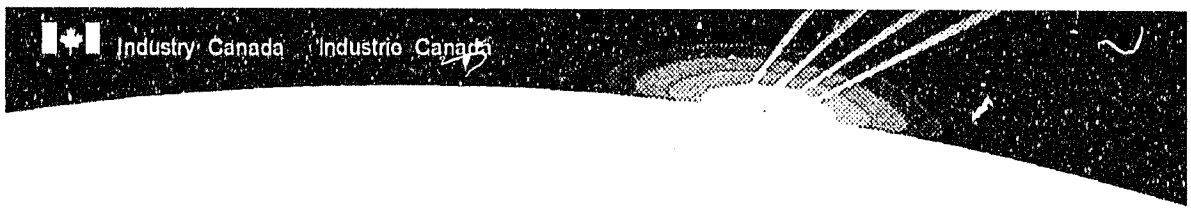

Audit of Industry Canada's Year 2000 Readiness

As of March 1, 1999

Canada

Executive Summary

Background

The Audit and Evaluation Branch (AEB) led an audit of Industry Canada's Year 2000 readiness in early 1999 to provide assurance to senior management that Industry Canada has taken all possible measures to be Year 2000 ready. To complete the audit seven criteria were assessed.

Findings

The Year 2000 project at Industry Canada is well advanced. Over the past several years significant progress has been made to achieve Year 2000 readiness at Industry Canada. To fully achieve Year 2000 readiness, more work is planned for completion by the end of the first quarter of 1999-2000.

To assess the work to be completed in the first quarter of 1999-2000, we recommend that a follow-up audit be conducted in the second quarter of 1999-2000.

A summary audit assessment against each of the seven audit criteria is provided below:

Criterion 1: Is the management control framework sufficient to adequately manage and monitor Year 2000 readiness?

The management control framework is sufficient to manage the Year 2000 project in the Department. A Year 2000 Project Office was established two years ago. Full-time staff in the Project Office provide guidance, awareness and quality assurance. In addition, progress towards departmental readiness is monitored and is reported to senior management monthly.

It is essential that the functions of quality assurance and monitoring continue to be high priorities for the Project Office. This will ensure key steps are completed to support Year 2000 readiness for all that have not signed off at December 31, 1998 such as: critical systems; high impact, small-scale applications; branches; and regions. (*refer to recommendation #2*).

Criterion 2: Is the list of critical systems complete?

Overall, auditors agreed that the 41 "critical systems" identified by the working group and senior management is complete. However, some applications labelled as 'high impact, small-scale application', such as the National Graduate Register and the Virtual Distributed Laboratory, were not included in the critical systems list. They have now been recognized as significant and are being managed like critical systems (*refer to recommendation #1*).

Criterion 3. Are critical systems Year 2000 ready?

Documentation adequately supported readiness conclusions drawn for the selected three critical systems, two branches and two regions signed off by December 31, 1998. The work necessary to achieve readiness for selected systems not signed off December 31, 1998 is being completed and documented. More work is required to demonstrate due diligence. Although the work of Year 2000 readiness of many systems was substantially finished at the time of this review, outstanding tasks are being monitored by the Project Office to ensure these are completed.

Any statements of Year 2000 readiness or compliance shown on the web site or other documents to clients, should be reviewed by Legal Services for potential exposures to liability (*refer to recommendation #3*).

Criterion 4: Are all assets affected by Year 2000 identified?

The majority of assets affected by Year 2000 have been identified. However, applications are still being added to the list. To minimize risk, the Project Office is also developing a separate list of internal dependencies and external interfaces linked to the applications that have been included in the inventories of critical systems, branches and regions. This addition list is deemed necessary to monitor that the critical, supporting infrastructure, upon which the applications depend, are Year 2000 ready. The Project Office is planning to identify and monitor internal dependencies and external interfaces in the next phase of the project. This will provide additional assurance that the systems are fully supported. (*refer to recommendations #4 and #5*).

Criterion 5: Have test plans been adequately planned and executed?

Test results for the critical systems selected that had signed off December 31, 1998 were documented. Strategies and test cases identified in the Year 2000 compliance kit were followed. Exceptions to the test strategies were noted and explained for such systems as the Integrated Financial and Materiel System (IFMS) and the Emergency Telecom Line Load Control System (LLC). These exceptions should be considered when contingency plans are prepared.

The Project Office should continue to assess the adequacy and completeness of testing each critical system and high impact, small-scale application not signed off at December 31, 1998 (*refer to recommendation #6*).

Criterion 6: Have contingency plans been prepared for critical systems?

Although some contingency plans have been identified for critical systems, they have not been completely developed, nor have the full impacts of failure been assessed. A process for preparing contingency plans is being developed. Specific procedures and responsibilities to address various

stages of failure, as well as escalation procedures, have yet to be identified. Contingency plans are required for all critical functions since failures could occur even though conversion was done appropriately and was tested. Such failures could significantly disrupt the delivery of key services (*refer to recommendation #7*).

Criterion 7: Have due diligence requirements been met?

Applications selected for audit that were signed off at December 31, 1998 have met the requirements for due diligence. In each case documentation supports the inventory assessed, approach taken and testing completed.

For systems not signed off at December 31, 1998, more documentation will be required to demonstrate due diligence (*see recommendation #2*). The Project Office is regularly monitoring progress informally and formally through the completion of monthly status reports. The status of readiness for critical systems; high impact, small-scale applications; branches and regions is assessed using a quality assurance process. Regular reports are provided to senior management informally and formally through presentations at senior management committees. At these presentations, high risks are highlighted.

Background

Industry Canada established a Year 2000 Project Office January 1997. At that time a representative from the Audit and Evaluation Branch joined the Project Office as a resource/advisor and participated in the working group meetings.

The project manager and working group identified 41 departmental critical systems included in 71 branches of the Department. The group also began to inventory customized off-the-shelf software; third party IT hardware and software; office equipment; real property; in-house developed hardware and software; and scientific/laboratory equipment.

The Project Office prepared monthly reports on the status of the 41 departmental critical systems for the Information Management/Information Technology and the Information Management Committees and the Department Management Board. This status report rated each critical system by using colour coding (white, green, amber and red) to show the progress toward Year 2000 readiness by the targeted date of December 31, 1998.

By the deadline of December 31, 1998, each branch head was asked to sign off on Year 2000 readiness by answering 56 pertinent questions based on the Industry Canada Compliance Kit. These answers had to be supported by summary sheets sent to the Year 2000 Project Office and by detailed supporting documentation retained in branch files.

Objectives

AEB conducted an audit of Industry Canada's Year 2000 readiness in early 1999 in order to provide assurance to senior management that Industry Canada has taken all possible measures to be Year 2000 ready. To achieve this objective, the following seven criteria were selected to ensure the following measures are in place:

1. *Project methodology and procedures* of the Year 2000 Project Office are sufficient to adequately monitor and evaluate Year 2000 readiness as attested by the sign off reports and supporting documents due December 31, 1998 by Branch heads;
2. The *list of critical systems identified* (41 in total), as well major categories of assets (e.g., CRC scientific/laboratory equipment) are complete;
3. *Critical systems are either Year 2000 ready* at December 31, 1998 or have good probability of being Year 2000 ready by June,1999 based on their project plans to meet stated milestones;
4. *All assets, not included in the 41 critical systems list, have been identified* as high impact, small-scale applications; customized, off-the-shelf software; third party IT hardware and

software; office equipment; real property; external interfaces; internal dependencies; and scientific/laboratory equipment and are Year 2000 ready as attested by the sign off reports and supporting documents;

5. *Test plans and results are appropriate* to assess Year 2000 readiness;

6. *Contingency plans* have been prepared where needed; and

7. *Due diligence requirements* have been met by the retention of Year 2000 project plans and related monitoring and project management reporting.

Approach

The approach included conducting interviews and examining key documents as noted below:

Interviews were conducted with key individuals, including:

- Project Office management and staff;
- managers responsible for critical systems selected; and
- regional and branch representatives

The following key documents were examined:

- Industry Canada publications covering the Department's mandate: *Industry Canada Performance Report for the period ended March 31, 1998* and *Industry Canada: Making a Difference – Our Priorities for 1998-99*;
- inventories, compliance strategy reports, test results summaries, compliance memos, completed questionnaires for selected applications, branches and regions that have signed-off at December 31, 1998 such as: Emergency Telecom Line Load Control System (LLC), Small Business Loan Administration (SBLA), Contribution Management Information System (CMIS), Prairies/NWT and Ontario Regions, Strategic Information Branch (SIB), and Office of the Superintendent of Bankruptcy (OSB);
- inventories, test strategies, progress reports for selected applications that had not signed-off at December 31, 1998 such as: IT Infrastructure - Wide Area Network (WAN), Newly Upgraded Automated Name Search (NUANS), Electronic Business Environment (EBE), and the Integrated Financial and Materiel System (IFMS);
- Year 2000 quality assurance checklist completed by the Project Office for those groups that have signed off at December 31, 1998; and
- Canadian Intellectual Property Office (CIPO) audit reports.

Findings

The departmental Year 2000 Project Office has focused its efforts on the high priority applications identified on the list of 41 critical systems. The focus will now also include applications labelled as 'high impact, small-scale applications'. To manage and assess the conversion of these small-scale applications, the Year 2000 Project Office plans to employ the same processes as were used to manage critical systems.

Criterion 1: Is the management control framework sufficient to adequately manage and monitor Year 2000 readiness?

There is an adequate management control framework in place to manage the Year 2000 Project in the Department. Progress toward departmental readiness is monitored and reported monthly to senior management. Key project management processes include the following:

- an organizational structure with consistent support from senior management;
- full-time staff in the Year 2000 Project Office;
- definition of Year 2000 compliance processes and deliverables;
- awareness training provided to staff through personal contact and workshops already completed for the critical systems as well as workshops planned for small scale applications;
- a quality assurance process conducted by the Project Office to ensure key steps are followed (inventory, testing, documentation) and appropriate sign-off are completed;
- a questionnaire designed to assess each reporting entity;
- activities conducted by the Project Office to ensure the completeness, consistency and validity of information supplied;
- consolidation and sharing of information through the Project Office (building systems, office equipment) for all areas affected by Year 2000 activities; and
- a system for identifying the progress of critical systems and branches (white, green, amber, red) which is also used for monitoring and reporting. This will also be used for high impact, small-scale applications.

Criterion 2: Is the list of critical systems complete?

The list of critical systems was identified through consultation and oversight of the departmental working group and senior management. To assess the completeness of Industry Canada's list of 41 critical systems, a comparison was made to the Department's mandate as outlined in the documents *Industry Canada Performance Report for the period ended March 31, 1998* and *Industry Canada: Making a Difference - Our Priorities for 1998-99.* The 41 critical systems were then grouped into the Department's performance goals and the results of the completeness audit were documented.

Some related systems that support the mandate, such as the National Graduate Register and the Virtual Distributed Laboratory, were not included in the list of critical systems. These systems have been identified as small-scale applications. The Project Office expects that any other system directly supporting a strategic objective of the Department will be identified through the inventory of small-scale applications currently underway.

There is a risk that some high impact, small-scale applications may not have been given appropriate attention. This risk is minimized since the Project Office plans to monitor, report and assess the high impact, small-scale applications using the same process used for the critical systems. It is expected that the efforts required to assess, convert, test and accredit small-scale applications will be significantly less than that required for critical systems. As such, the Project Office expects that the high impact, small-scale applications will be converted and tested by May 1999.

Some critical systems identified were assessed as having little or no impact of failure and may not need to be on the critical list. However, risk assessments were conducted on the list of critical assets based on specific criteria and weightings. To support their inclusion on the critical list, the Project Office determined that these systems could cause political embarrassment should system fail.

Recommendation

It is recommended that the Project Office:

1. *ensure that systems identified as high impact, small-scale applications are managed and monitored like critical systems.*

Criterion 3: Are critical systems Year 2000 ready?

A sample of seven of the 41 critical systems (three had been signed off as of December 31, 1998 while four had not), two branches and two regions were selected for audit purposes. Selection was determined through a process of conducting discussions with responsible managers and reviewing documentation. Auditors also reviewed the implementation of recommendations made from the Year 2000 audits at the Canadian Intellectual Property Office completed on two systems - Intrepid II and Techsource. The Project Office accepted Year 2000 sign off when most of the Year 2000 compliance requirements were completed but continues to monitor these outstanding tasks.

Key audit findings for this sample are presented in the sub-sections below.

Critical Systems, Branches and Regions signed-off by December 31, 1998

Critical Systems

The three critical systems selected (which were signed off at December 31, 1998) are:

- Emergency Telecom Line Load Control System (LLC);
- Small Business Loans Administration (SBLA); and
- Contribution Management Information System (CMIS).

These systems did not require significant code conversions since all were designed using a four-digit year. Compliance testing for each of the above systems is documented and complete. Millennium testing was completed in an environment separate from production. The departmental compliance process was followed and documented. The LLC system includes a compliance statement on the web site that was not reviewed by Legal Services for potential exposures to liability.

Regions

The two regions selected which were signed off at December 31, 1998 are:

- Prairies/NWT Region
- Ontario Region

Prairies/NWT Region

The Prairies/NWT Region signed-off as Year 2000 ready although there were outstanding items that have since been addressed (such as the two high impact, small-scale applications). The other item will be completed by the strategy mentioned below by March 31, 1999. Documents supported the work done and conclusions reached for Year 2000 readiness.

The region is geographically dispersed requiring significant co-ordination in developing inventories. Most of the assets are third party IT hardware and software. This required standard testing tools and vendor confirmations. Students from the First Step program were hired to develop inventories and test PCs for compliance. No system interfaces were identified.

The deadline for the regional strategy for compliance is March 31, 1999. Regional staff are required to either replace, discard, or develop a work-around for any items not Year 2000 compliant. Users are required to verify compliance for off-the-shelf software products that differ from the departmental standard since non-standard software not compliant will be removed from the servers. The region is relying on central groups to verify and test compliance of the Industry Canada standard software products.

Two high impact, small-scale applications were identified: the Lindex and Aptrac. These applications have been tested and the supporting documents are being reviewed for quality assurance by the Year 2000 Project Office.

Ontario Region

The Ontario Region signed off as Year 2000 ready at December 31, 1998. Documents were in place to support the work done and conclusions reached.

Most of the assets were third party IT hardware and software. This required standard testing tools and vendor confirmations. Some stand-alone data calculation applications have been developed in-house. During the inventory exercise, business managers were asked to identify all hardware and applications used, assess the importance of these applications as well as their date dependency. They were asked to remove applications if not needed. This exercise resulted in many small applications being removed. The region is relying on central groups to verify and test compliance of key departmental applications (e.g., Spectrum Management System, CMIS, IFMS and WAN infrastructure) as well as the Industry Canada standard software products.

One high impact, small-scale application was identified, Technical Measurement Reporting System. This application is being managed by the Spectrum Information Technology and Telecommunications Sector.

Branches

The two branches selected for audit purposes signed off at December 31, 1998 are:

- Strategic Information Branch
- Office of the Superintendent of Bankruptcy

Strategic Information Branch (SIB)

With the exception of the Strategis application, reported separately as a critical system, SIB signed-off as Year 2000 compliant. Documents were in place to support the work done and conclusions reached for Year 2000 compliance. Most of the assets are third party IT hardware and software. This required standard testing tools and vendor confirmations. No interfaces or dependencies were identified. Summaries of test results were provided.

One high impact, small-scale application was identified - the GEAC Advanced Library System. This will be tested in the next phase of the project. It is planned that new computers will be acquired in March with testing and implementation of the Library System in April/May 1999.

Office of the Superintendent of Bankruptcy (OSB)

Documents were in place to support the work done and conclusions reached for Year 2000 readiness. OSB assets consist mainly of personal computers, laptops, printers, and various off-the-shelf software products. Two OSB critical systems, IMPACT and Insolvency Name Search, were assessed and reported separately. They were signed off and accepted by the Project Office at December 31, 1998. Test results were summarized.

OSB has identified one high impact, small-scale application, the Unclaimed Dividends Search (on Strategis), which will be millennium tested, if required, in the next phase of the project in the Chief Information Office Year 2000 test lab within the Strategis environment. Some OSB off-the-shelf products have been identified as "not Year 2000 compliant", although compliant versions are expected to replace existing products.

Critical Systems not signed off by December 31, 1998

Four critical systems selected for the audit were not signed off at December 31, 1998 are:

- IT Infrastructure - Wide Area Network (WAN),
- Newly Upgraded Automated Name Search (NUANS)
- Electronic Business Environment (EBE)
- Integrated Financial and Materiel System (IFMS)

IT Infrastructure - Wide Area Network (WAN

The process to ensure Year 2000 readiness for the WAN is well underway. Completion of asset replacement and testing is planned before the end of March 1999. To date, there is limited formal documentation of the procedures followed to ensure Year 2000 readiness. For example, there is no documented project plan or test strategy. However, the responsible manager plans to prepare a Compliance Strategy Report to provide adequate support.

Any Year 2000 impact analysis for the WAN is limited to identifying the components affected if a given asset fails. There is no attempt to measure the impact to the business areas that use the WAN as this is seen as the responsibility of each business area. Contingency planning is scheduled for completion by March 31, 1999 and will include increasing the level of redundant network components to decrease the likelihood of outages due to asset failure.

Newly Upgraded Automated Name Search (NUANS)

Industry Canada is the owner of the NUANS system. It is used for processing corporate and business name searches for new companies before incorporation. Industry Canada has a contract

with Digital Equipment of Canada (DEC, a subsidiary of Compaq Canada Inc.). DEC is given the right to use the software and has the responsibility to service the databases and provide access to various subscribers. Industry Canada is responsible for ensuring Year 2000 readiness of NUANS. DEC is responsible for ensuring that the technical infrastructure on which NUANS operates is Year 2000 ready.

NUANS is not yet Year 2000 ready. A contractor (Progestic International Inc.) has been hired to perform analysis and code conversion. Management indicates that the code analysed to date requires few code changes. Code conversion is due to be completed by April 20, 1999. A test strategy has been documented and test plans are being developed. A separate Year 2000 test environment has been created for NUANS where system dates can be manipulated to ensure all mandatory test dates are tested. Testing has begun and will continue for the next few months. As per the NUANS Year 2000 project plan, completion of the Compliance Strategy Report and the Compliance Memo are due June 30, 1999.

Electronic Business Environment (EBE)

The EBE system is managed in the Corporations Directorate of Industry Canada. It is a repository of Canadian corporate information that is received by fax and is manually input. The EBE is a phased development project which will replace the current non-compliant system known as Disco. The original target date for implementation of December 31, 1998 was delayed to March 31, 1999 due to scope changes.

The EBE development project is supported with appropriate documentation including the work done on Year 2000 readiness. Plans are monitored and controlled to meet the target implementation date of March 31, 1999. The readiness approach was guided by the Industry Canada and Human Resources Development Canada strategies. Acceptance testing is now complete and Year 2000 testing will begin February 22, 1999. EBE interfaces with two main systems: the AR/T2 transfer of Revenue Canada data from a tape, and the Dissemination application that transfers files produced by EBE to external sources such as NUANS. Both of these interfaces are compliant but have not yet been documented.

With continued monitoring of plans, it is reasonable to expect that Year 2000 readiness of EBE will be completed by the end of March 1999 (EBE signed-off March 31, 1999.)

Integrated Financial Management System (IFMS)

IFMS includes four areas: the generic SAP R/3 software; the Industry Solution/Public Sector (IS/PS) components implemented by Industry Canada and other government departments; the Receiver General Interface (RGI); and the interfaces with other departmental systems. The Treasury Board "Core" group, of which Industry Canada is a partner member, is assuming

responsibility for Year 2000 testing of upgraded versions of the IS/PS and RGI. IFMS Core is relying on vendor certifications for the SAP R/3 application given world use and low risk. Each department is responsible for testing its own interfaces for continued compliance. It is expected that once the tested upgrades are implemented, and since no code changes will be made in Industry Canada, Year 2000 compliance testing is not required. Nevertheless, the Treasury Board "Core" group recommends some departmental Year 2000 testing.

Limited testing was conducted on the interfaces where data formats were reviewed for files transferred between systems. Full millennium testing on a Year 2000 environment was not considered possible due to difficulties in the infrastructure architecture. The difficulties were fully documented and a formal recommendation was made by the Comptroller's Branch and was accepted by the Project Office. The need for re-testing interfaces with the upgraded versions of IS/PS and RGI has not yet been assessed.

Core testing is not being done on an infrastructure similar to the one used in Industry Canada. This risk is reduced by vendor confirmation of Year 2000 compliance of the departmental infrastructure that supports IFMS.

Review Implementation of Recommendations per Audit Reports

Canadian Intellectual Property Office (CIPO)

Audits of Year 2000 readiness were conducted in 1998 on two CIPO critical systems - Intrepid II and TechSource. Auditors reviewed the progress of implementing recommendations made by these two previous audits and found that they have been, or are currently being, implemented by Informatics Services Branch (ISB).

The interim audit report on Intrepid II, dated June 1, 1998, with an update dated June 22, 1998, recommended that additional compliance documents be gathered and that copies of relevant documents be provided to the Project Office. Based on information provided in the update and discussions with the Project Office, these requirements have now been met.

The final audit report on TechSource, dated September 23, 1998, identified five recommendations. A follow-up action plan, dated December 1998, was prepared to address the audit recommendations. The main recommendation has been addressed. It relates to improving testing documentation and scripts for the application component and ongoing conversion, and re-running tests to establish a baseline for Year 2000 testing of new releases. ISB has agreed to upgrade its documents to ensure that the same tests can be conducted on the next release and mid-life refit of TechSource. This will be the last upgrade until March 2000 as ISB plans to freeze any further releases of TextSource from September 1999 to March 2000. The other audit recommendations have been met or will be addressed within the context of Industry Canada's Year 2000 contingency planning framework.

Recommendations

It is recommended that:

2. *the Project Office continues the functions of quality assurance and monitoring until all areas are signed off as Year 2000 ready. This will ensure key steps are completed to support Year 2000 readiness for all critical systems; high impact, small-scale applications; branches and regions that have not signed off at December 31, 1998; and*
3. *public statements of Year 2000 readiness (such as the statement made for LLC on the web site) be reviewed by Legal Services to minimize potential exposure to liability.*

Criterion 4: Are all assets affected by Year 2000 identified?

Many types of inventory are being identified and assessed for Year 2000 compliance. This is being done in accordance with Project Office documentation and quality assurance requirements. Inventories from the regions and branches include the following areas: applications (critical and small-scale), office equipment, vehicles, real property, scientific and test equipment, and internal dependencies and external interfaces.

The Project Office had requested that external interfaces be identified. Staff feel they have been properly addressed for critical systems. Many external interfaces are paper based (e.g., SBLA) or manually entered by partners (e.g., LLC). However, the level of risk, in terms of volume or complexity, is not well understood for small-scale applications. The Project Office intends to address these issues in the next phase of the project.

Dependent Infrastructure

In addition to assessing Year 2000 readiness for applications, the supporting infrastructure upon which these applications depend must also be compliant. This will ensure continued delivery of the service or product. Where groups assumed that others are addressing their internal dependencies, assumptions have been identified and reviewed by the Project Office for reasonableness. For example, the IFMS conversion team is relying on a separate group to confirm compliance of the operating infrastructure (RS6000, operating system, LAN, database system, desktops, etc.). Although the Project Office assesses the reasonableness of the assumptions, documentation does not exist to identify and cross-reference all internal dependencies on a global basis.

The Project Office is planning further follow-up of assumptions in the next phase of the project. It is expected that further clarification of the business functions will be provided through the contingency plan project currently underway. This information will be used to cross-reference all dependent components for each business function.

Recommendations

It is recommended that the Project Office:

4. *document and carry out plans to follow-up assumptions and internal dependent components for each business function. This should include considering cross-referencing assumptions and internal dependencies for each business function.*
5. *continue with plans to assess the risks involved with external interfaces for the high impact, small-scale applications.*

Criterion 5: Have test plans been adequately planned and executed?

Test results for the selected critical systems were documented and followed the strategies and test cases identified in the Year 2000 compliance kit. However, the following exceptions were noted and explained:

- Testing was not done in a Year 2000 environment for IFMS, as previously described, due to the difficulties with the infrastructure.
- SBLA initially did not test on a separate Year 2000 environment but later did so at the specific request of the Project Office.
- Interfaces were not tested using live data for IFMS due to the difficulties in replicating a test environment. Due to the lack of changes made, the interface of LLC with telephone companies was not tested in co-operation with its partners.
- Regression testing was not required in many cases since many systems did not require any code changes resulting in not changing existing functionality, e.g., SBLA and CMIS.

Recommendation

It is recommended that the Project Office:

6. *continues to assess the completeness of testing conducted for all areas not signed off at December 31, 1998.*

Criterion 6: Have contingency plans been prepared for critical systems?

A plan, including milestones, for preparing contingency plans is being developed by a Year 2000 Business Continuity Project Steering Group of departmental senior management. They will manage the completion of the contingency plans deemed necessary. A detailed assessment of impacts is being requested from all responsible business and technical managers

Some contingency plans have been identified for the critical systems at a high level (e.g., use of manual processes, securing of technical resources). However, these plans have not been fully developed nor have the impacts of failure been fully assessed for each critical system. Specific procedures and responsibilities to address various stages of failure as well as escalation procedures have yet to be identified. For instance, system failure of a day could be addressed satisfactorily through manual procedures. However, system failure of two weeks may cause problems such as significant backlogs, cheques issued late or inaccurate records. Senior management decisions for investments or external communications may be required at various stages of failure. Once developed, contingency plans must be tested and individuals must be trained in the procedures.

Contingency plans are required for all critical functions as failure can occur even when conversion and testing efforts have been properly conducted. A failure in critical functions would significantly disrupt the delivery of key services.

Recommendation

It is recommended that the Project Office:

7. *continues to monitor and participate in efforts to develop contingency plans for individual business functions to ensure that plans are well developed to match the varying impacts of failure. In addition, contingency plans must address all components used to deliver the function, e.g., hardware, applications, external interfaces, internal dependencies, and infrastructure. Contingency plans should be tested and staff trained to ensure the plans are efficiently executed when needed.*

Criterion 7: Have due diligence requirements been met?

For those applications selected that have substantially completed Year 2000 readiness requirements, documentation showing the assessment of inventory, approach taken and completion of testing supports due diligence requirements.

As noted under Criterion 3, relating to those areas that have not signed-off, documentation will be required to demonstrate due diligence (*refer recommendation #2*). The Project Office should assess this documentation for completeness and reasonableness when sign- off is received.