Government of the Northwest Territories

PeopleSoft Implementation Review

July 16, 1999

TABLE OF CONTENTS

Executive Summary

The Government of the Northwest Territories ("GNWT") recently completed the customization and installation of a PeopleSoft™ HRMS system for Human Resources Management, Payroll, and Time and Labour modules; ***the Polar Project***. Under contract with the Audit Bureau of the Financial Management Board Secretariat for GNWT (the Audit Bureau), dated June 23, 1999, we at Grant Thornton carried out a 'PeopleSoft Implementation Review' of the Polar Project. This report details the findings of our review.

A summary of this report follows.

1. Scope

The GNWT's Polar Project consisted of implementing Commercial - Off-The-Shelve PeopleSoft applications with approximately 75 internal customizations. A project team comprised of GNWT and SHL Systemhouse (SHL) staff and directed by a full time SHL project manager carried out the implementation project. A complete Project Work Plan was established and the project team reported to a Working Committee. The 'go live' implementation date occurred July 9, 1999. The PeopleSoft application provides one integrated Human Resource Management and Payroll System for approximately 3,500 employees in the GNWT, the NWT Housing Corporation, and the Stanton Regional Hospital, communicating over a Digital Satellite Communication Network.

The director of Labour Relations & Compensation, the Peoplesoft Implementation Team, and the Peoplesoft working committee asked for assurance that all key aspects of control in connection with this PeopleSoft Implementation were incorporated into the PeopleSoft system in a timely manner. Specifically, it was recognized that control issues exist within several aspects of this project including the applications themselves, the general computer control and security environment, legal requirements, implementation, systems operations, other application interfaces, data management and disaster recovery planning. Accordingly, the Audit Bureau contracted Grant Thornton, as experienced Peoplesoft consultants and auditors, to carry out a broad-based assessment of controls and information system security and identify deficiencies within these systems and the implementation project.

Specifically, the implementation review carried out the following:

Key Application Controls
- ✓ review business process blueprints and scripts and simulation phases;
- ✓ communicate with management to assess the controls designed in the application
- ✓ carry out the process control review and testing to ensure controls would mitigate any control weakness

Application access/authorization security
- ✓ review high level job roles for potential segregation of duties issues
- ✓ review mapping of authorizations to job roles and reporting on any segregation of duties issues or sensitive profiles resulting from the mapping process.
- ✓ analyse high risk system delivered profiles assigned to users in the production environment
- ✓ analyse user's access to sensitive transactions and back door exits to the operating system
- ✓ analyse User Master Records for appropriate segregation of duties between incompatible transactions and identifying any powerful users, which all should be tightly controlled.

Infrastructure Security
- ✓ review the security within the operating systems, network(s) and the relational data base management system.
- ✓ review the plans of how program and table updates are promoted between the defined Peoplesoft development and test instances and their related production clients.

Functional requirements and fit analysis
- ✓ review of GNWT and related agencies' authorities such as the Financial Administration Act, Public Service Act, Human Resource Manuals, Collective Agreements, and any other personnel and payroll related authorities to ensure that the data selected for the systems meets users expectations
- ✓ reports required by system specifications
- ✓ adequacy of systems documentation

Change control processes
- ✓ review change control processes to ensure their integrity and security.

Implementation integrity
- ✓ review of conversion strategy
- ✓ project management disciplines
- ✓ conversion plans and the design of the procedures
- ✓ data cleansing procedures
- ✓ data reconciliation processes

Manual, clerical and supervisory controls, management procedures, and training strategies/programs/procedures for ensuring the continued operation of the system and its basic controls over inputs, outputs and processing of data (Retitled 'Operational Controls' for this report)
- ✓ on-going maintenance of system

Security and integrity of application interfaces
- ✓ review of application interfaces with financial information systems of GNWT, NWT Housing Corporation, and Stanton Regional Hospital to ensure adequate levels of security and integrity

Storage and retention requirements of data

Disaster recovery plan

Our review procedures do not constitute an audit for the purpose of expressing an audit opinion on whether the PeopleSoft systems operate in a manner that ensures the confidentiality, integrity and availability of information and processes for which they were designed. Rather, our review procedures were carried out to assess the existence and effectiveness of internal controls and information systems security designed into these systems in order to identify and report deficiencies that have come to our attention.

2. Our Work Effort

Grant Thornton carried out a broad-based review of all of the areas outlined above. Our review was structured to evaluate controls and security against the scope requirements of this assignment and wherever possible 'best practices' standards. Details of our work effort is as follows:

Resources and Timing
Our review was carried out by a senior four person field team reporting to Doug Cruickshank, Partner responsible for the IT Risk Management group of our B.C. regional practice. These four consisted of three Grant Thornton professionals and one member of GNWT's Audit Bureau who provided a complementary mix of skills and experience to satisfy all aspects of the assignment. Specifically, the audit team provided expertise in:

- Both the functional and technical aspects of Peoplesoft HRMS and Payroll applications
- Applications controls assessment and audit
- Computer general control assessment and audit
- PeopleSoft project management and implementation
- Financial and regulatory compliance

Two field visits were conducted. The first visit, June 21 - June 25, consisted of orientation and preliminary information gathering. The second field visit, July 5 – July 16, consisted of detailed information gathering, testing and analysis. Following further analysis, the findings and our recommendations have been laid down in this report.

The Review Process
The review process consisted of the following:

1. develop a review plan that addresses the specific control objectives identified in the project scope,
2. execute the procedures of the review plan,
3. identify and report control and security weaknesses,
4. report constructive recommendations for changes.

The Report

Following this summary is the detailed findings and recommendations for each area reviewed. Our report sets out the following information in each of these sections:

Preamble	To provide, when useful, background information associated with the area under review
Review Objectives	The assurance objective(s) in connection with this aspect of the review.
Review Procedures	Detailed procedures carried out to satisfy assurance review objectives.
Findings and Recommendations	Our observations on control deficiencies and other matters and our associated recommendations to improve these deficiencies. As well, we have ranked the 'significance' of our findings as either 'high', 'medium' or 'low', based on our judgement of the risks inherent in the finding.

3. A Summary of Findings

Our review identified numerous matters that we have detailed within this report. A summary of our overall observations arising from our review follows:

(a) We are concerned about the extent of weaknesses found in information system security surrounding the PeopleSoft applications. These weaknesses exist at various levels of the computer systems, including the Wide Area Network ("WAN"), the Local Area Network ("LAN"), the PeopleSoft HRMS application, the HP UX operating system, and the Oracle database. These weaknesses pose a serious threat to the confidentiality, integrity and availability of the Government's information systems and we have made several recommendations within the report for these items. These weaknesses are exacerbated because there isn't an information systems security program to direct security matters across all government departments and agencies. GNWT should develop an organization-wide Enterprise Security Program (ESP) that directs users, operators and developers on all standards of security expected for its information systems.

The fundamental activities involved in an ESP are:

- Assessing system security risks and determining appropriate safeguards;
- Developing a comprehensive System Security Policy;
- Developing System Monitoring Policies and Practices;
- Developing an Incident Response Plan; and
- Developing and implementing a Security Awareness Program

(b) We believe there was a lack of appropriate communication between the Public Works & Services department and the PeopleSoft Implementation Team. In particular, as the implementation phase draws to a close, we are concerned about the transfer of knowledge from the PeopleSoft team to the database administrator in the Public Works Department. At the time of our fieldwork, the knowledge transfer had not taken place. The database administrator is a key role within the PeopleSoft support group and it is crucial that he is knowledgeable, comfortable with the system and able to carry out his duties as the database administrator. Consequently, we recommend that this activity take place well before the PeopleSoft Team database administrators' contract expires on August 20th.

(c) We found that most PeopleSoft implementation team members had full access to the production programs and data. Consequently they have the ability to run a payroll, change records directly without having to add a new record and modify their own payroll records. Security and program change control dictates segregation of duties that isolates programming from the production environment. We have made several recommendations to improve security and change control processes to address this matter.

(d) We found the disaster recovery plan to be limited in scope, requiring more rigorous planning. Further, staff need to be trained in disaster recovery procedures and the disaster recovery plan needs to be tested thoroughly. Ideally, a disaster recovery plan for the Payroll and Human Resource functions should be integrated with the other disaster recovery plans of the government.

(e) Judging from our experience on other implementation projects, we found it unusual that the project manager would leave the project, so soon after the "go live" date. Considering the significant time, financial resources, and effort expended on the project, we felt that it would have been prudent for the project manager to remain on for at least two full pay periods following the "go live" date.

(f) Many aspects of GNWT departments and agencies are significantly decentralized. For the sample of government departments we reviewed, we found that LAN systems, administration and security varied considerably and there was no consistency in segregation of duties between departments. We believe the Government should develop policies and standards dealing with these issues in order to ensure consistency.

(g) The documentation prepared by the PeopleSoft Implementation Team was excellent. It was complete and thorough in almost all cases. The level and quality of documentation for this project is something we would like to see all of our PeopleSoft clients strive towards.

Conclusion

While we have identified a significant number of matters that require attention, we also note that the first payrolls since the 'go live' date have been successfully delivered from the new systems. A significant amount of work has been carried out by GNWT's PeopleSoft Implementation Team to accomplish this feat. Obviously, the initial success is an important indicator of the integrity and reliability of the system. However, we emphasize management must be diligent in maintaining adequate internal controls and security and encourage prompt attention to our findings and recommendations.

At this time we wish to advise that the GNWT staff and consultants whom we worked with were extremely helpful and forthcoming with information. This cooperation significantly contributed to the efficiency of our work effort and the quality of our findings and recommendations. We sensed a high level of commitment amongst staff to get the job done right and applaud the Implementation Team and all others who assisted us carry out this review.

A. Key Application Controls

1. Review of business process blueprints, scripts and simulation phases

Preamble

A customized PeopleSoft User Manual was developed to assist in functional training and to document user procedures. This manual is referred to as the "Human Resource Management System" and was distributed to the users during training for reference when using the PeopleSoft application. The manual is to be finalized and re-distributed in September 1999. Future plans for the maintenance and distribution of the manual call for this material to be available on the GNWT web site. When changes occur, the web site documentation is to be updated and the User Community will be notified to visit the site and download the latest version. The longer-term plan is to incorporate GNWT procedures directly into the PeopleSoft on-line help.

The manual contains the following sections:

1. Objectives
2. Table of contents
3. Agendas referencing the process and page number for each section
4. Flowcharts
5. Navigation Map (spreadsheet of panel or report name & data available)
6. Introduction
7. Terminology
8. Paths & panel prints
9. Discussion in addition to the step by step
10. Checklists to think about what other processes may affect this

Review Objectives:

- Assess whether Payroll and Human Resource management business processes embodied within the PeopleSoft user documentation is complete and effective.

- Assess whether this documentation is easy to follow and offers consistent procedures to all users.

Review Procedures:

1. Check that all referenced sections listed on the User Manual Table of Contents exist and include procedures for each module implemented.
2. Evaluate the business processes contained within the User Manual for completeness and effectiveness.
3. Select sample of procedures and using test data and a selection of user accounts, determine if the documented procedures are accurate and adequate to satisfy user requirements (i.e. to understand the system and to accomplish business objectives).

Findings and Recommendations:

Ref#	Findings	Recommendation	Significance
A.1.1	At the time of our fieldwork, the manual was still in the process of being finalized. Details are as follows: A Benefits Reports Section was listed in the Table of Contents but was not found in the original User Manual provided for examination. Note: The section was provided upon request. It had been sent out on June 24,1999 to users. The Tables Section had no documentation. A special Folder for Table's was found in the PeopleSoft Directory located on the network server storing the electronic version of the User Manual. The Budget and Encumbrances Section was empty and delivered to us subsequently. Note: An overview document was sent to the Director(s) of Finance near the end of June, 1999 to prompt for trainees to attend sessions in this area scheduled for August, 1999. The process itself will not be rolled out until testing is completed via several live payrolls. This is a good approach to take because it is not an easy process to maintain within PeopleSoft and thorough testing and careful roll is appropriate.	Unfinished aspects of the User Manual and the associated business processes should be completed before the Implementation project is determined finished.	Low
A.1.2	The User Manual documentation lacked some rigor for referencing between the	The User Manual should make reference to and	Medium

Ref#	Findings	Recommendation	Significance
	manual process and the application. Specifically, a sample of each manual input form was not included in the applicable sections to aid users relate the input form and the associated on-screen panel.	include a sample of applicable completed input form(s), by procedure to document the transposition of data from hard-copy manual input forms to the equivalent on-screen panels.	
A.1.3	We could not locate in the User Manual a listing of helpdesk resources. We noted the users had been issued a mouse pad with help desk phone numbers. While this is an innovative approach, it cannot readily be updated as could be a Manual.	The User Manual should include a page on "who to call for what" and the associated contact local numbers or email addresses (i.e. helpdesk).	Medium
A.1.4	The User Manual was sometimes missing page titles that reminded users of the context for the information that is documented on a particular page. Specifically, a page title to identify the type of Business Process being documented should span all pages that document that process.	We recommend a transaction title be added to the standard format on each page (i.e. New Hire) to help the user relate to the information contained on any particular page, especially in cases where procedure spans several pages.	Low
A.1.5	There is no documented process for updating the User Manual, especially in circumstances where users identify documentation errors.	The Manual should include a section advising users on what to do if an error is noted in the Manual.	Medium

2. Review of Internal Controls Built into the Application

Review Objective:

Evaluate adequacy of application controls of the PeopleSoft system.

Review Procedures:

- Benchmark internal controls designed into the GNWT implementation of PeopleSoft HRMS version 7.0 system against the Canadian Institute of Chartered Accountants (CICA), 'Information Technology Guidelines' for Application Based Controls[1] and the Grant Thornton InFocus™ Controls Evaluation methodology.
- Test effectiveness of application controls using a test database for major processes as follows:
  - Hiring
  - Employment Termination
  - Time entry (Time and Labour)
  - Changes to Employee records (promotion, raise, transfer, etc)
  - Payroll Payment
  - Recording of the Payroll in the General Ledger
  - Paid Leave Administration (Vacation, Sick Pay, Overtime recovered)
  - Benefits Administration

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
A.2.1	A warning is issued if the SIN of a new hire matches that of an existing employee when entered, but the user is allowed to proceed with setting up a new record. Further, the program will permit payroll disbursements for the new hire bearing a duplicate SIN of another employee.	The system should be modified so that a user cannot set up a new hire if the SIN matches that of an existing active employee.	Medium

[1] CICA, Information Technology Control Guidelines, 3rd Edition, Control Object DD

Ref#	Findings	Recommendations	Significance
	Note: The system does prevent new hires from being created if an invalid or null SIN is entered.		
A.2.2	Human Resource staff with rights within PeopleSoft to hire employees are not restricted to hiring for their department only. Any employee who has hiring rights within PeopleSoft can setup a new employee and assign them to any department within the Government. We recognize that once created , the new employee's record can not be accessed if they belong to another department, however, due to the risk of collusion we have included it as a finding.	The system should be modified so that Payroll and HR personnel are restricted from hiring staff in any other departments. Until this recommendation is implemented, each HR manager should receive an exception report for each payroll showing changes made to employee records by someone outside the department.	Medium
A.2.3	Similar to Item# A.2.2, payroll clerks can enter, change or approve time posted for employees in any other department, and not just those within the departments they administer. This is an inherent control weakness with PeopleSoft HRMS Version 7.0 Time and Labour Module.	We recommend an upgrade to PeopleSoft HRMS version 7.5 that addresses this control weakness. In the interim, we recommend that an exception report showing time and labour entries that originate from a payroll clerk outside the department is provided for each payroll to the departmental HR Manager for review.	High
A.2.4	Users cannot change their own payroll and HR records on the system. The application's Security Administrator associates user ID's with their employee number and denies update privilege to any record with that user's employee number. We discovered that the project team had not entered their own employee numbers into the application's Security Administrator and consequently they are able to modify their own payroll and HR records.	The PeopleSoft implementation team employee numbers should be entered into the Security Administrator utility to restrict update access to their own payroll and HR information.	High

B. Application Access / Authorization Security

1. Security Design

Preamble:

The implementation of PeopleSoft application security was established via the systematic identification of access rights that are documented as follows:

- PeopleSoft Implementation Security matrices outline panel access security by security class (i.e. HR Administrator).
- A Security Set-Up matrix documents menus, panels, and reports by module and user class (i.e. Departmental HR) set as 'Hide' to deny access.
- A document details Security Classes documents the security class, members of that class and the type of processes permitted within modules and panels.
- A PeopleSoft User Security List matrix documents the pay office / department, location, name, sin, user ID, user class, and description of authorized users.

Review Objective:

To ensure the PeopleSoft implementation Team designed application access that established adequate segregation of duties amongst authorized users.

Review Procedures:

PeopleSoft Implementation Security (black books)

- Review at a high level the classes, panels and types of access documented for adequate segregation of duties for user classes.
  Note: Select a user class from this document, match with a user ID from the PeopleSoft User Security list and follow through on-line to see if access is setup as documented.

Security Set Up Matrix

- Scan this document for permissions not in compliance with adequate segregation of duties.
  Note: Consider guidelines established by the Polar Project Team.

Security Classes Matrix

- Scan this document for panel and report access permissions not in compliance with adequate segregation of duties.

PeopleSoft User Security List

- Select a sample of user ID's from this list and test the accuracy of this documentation by simulating a variety of access attempts on a copy of the production database.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
B.1.1	The user ID selected and tested (NWTHC employee) had more access on-line than what was documented on the matrix. However, the additional panels or reports did appear to be appropriate based on the role this user has.	Documentation supporting access rights with the PeopleSoft applications should be kept up-to-date by the PeopleSoft Security Officer. Periodic, independent reviews of the documentation should be carried out to confirm the rigor of the administration of PeopleSoft access security.	Medium
B.1.2	The Security Set-Up matrix shows that "Payroll – Central – FMBS" has access to the "Process" payroll panels that grant this user group privilege to execute payroll and print all reports. Per the Project Functional Team Leader, this privilege was not intended and has not been implemented. (i.e. CSS will continue to run the payroll jobs and they will not give the "Process" panels to Payroll) Consequently, the documentation is inaccurate.	Same as Item# B.1.1 above.	Medium
B.1.3	The Crystal Reports specialist was found to have two user ID's and "Add/Update/Correction" privileges. His Job classification suggests that for adequate segregation of duties this person should be granted "Read" privileges only.	Users should be limited to single user ID's to facilitate security administration and report specialists should not be granted access other than "Read" privileges.	Medium
B.1.4	We could not locate documentation evidencing the access rights assigned to the PeopleSoft Implementation Team.	To foster a rigorous administration of application level security, all users of the	Medium

Ref#	Findings	Recommendations	Significance
		PeopleSoft application should have their access rights identified and documented for periodic review and verification.	
B.1.5	We noted that most members of the PeopleSoft Implementation Team had been granted access rights to run Payroll and 'correction', which permits users to change records without inserting a new entry (loss of audit trail).	Adequate segregation of duties requires that system administrators and developers should not have unrestricted access to application functionality.	High

2. PeopleSoft Logical Security

Review Objective

To ensure PeopleSoft functionality provides adequate logical security to the application.

Review Procedure:

- Benchmark PeopleSoft application functionality for password administration against the CICA's, "Information Technology Guidelines' for 'Best Practices for Using Passwords'[2]

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
B.2.1	PeopleSoft HRMS Version 7 has poor password administration functionality. In particular we noted the following weaknesses: • There is no password minimum length (CICA recommends 8 characters minimum). • Forced password change on initial log-on not available (11 of 20 user Ids examined had not changed their passwords from that of their user ID assigned by the project implementers). • Permits reuse of passwords • Forced password change after a period of time not available. • Recognizable character sets are not prevented. • User lock out after a repeated failed login attempts not available (usually is 3 consecutive attempts).	We recommend an upgrade to PeopleSoft HRMS version 7.5 that improves password based access security. In the interim, we recommend that the PeopleSoft Security Officer develop and distribute password policies that require users to comply with the password practices we identified as weaknesses in this finding.	High
B.2.2	There are several security features within the PeopleSoft application which have not been used. These include: • The PeopleSoft Security Report that lists all users and access rights to modules, panels and menus for periodic review. • Setting Object Security that controls user access to change or update any	The security functionality within PeopleSoft should be used to the utmost advantage. In this connection, we recommend that the PeopleSoft Security Officer receive training in the security aspects of the application (PeopleSoft has	High

[2] CICA, Information Technology Control Guidelines, 3rd Edition, Appendix 6-1

Ref#	Findings	Recommendations	Significance
	object in the PeopleSoft security tables. ▪ Query Security which limits a user's access to only those data records that are defined by the Query Security search record that is linked to the record definition. ▪ PeopleSoft 'nVision' (a PeopleTool used to create queries that populate MicroSoft Excel Spreadsheets for use in building reports or performing detailed data analysis) security to control read access to data.	special courses for this purpose) and general application security administration.	
B.2.3	As at July 15, 1999 (last day of field work), we noted that members of the project's consulting firm, SHL, were still active users on the system although they were no longer working on the project	We recommend that the Project Implementation Team review the process for the prompt identification of terminated users and ensure this process operates effectively.	High
B.2.4	The password for Psoft, a highly powerful user account, is known by several members of the PeopleSoft Implementation Team and, although changed from the shipped default, it has not been changed regularly.	Superuser accounts like Psoft should be tightly controlled. Limited knowledge of the associated password and frequent password changes using good password practices is recommended.	High

C. Infrastructure Security

Preamble:

For the computing environment for the PeopleSoft 3 Tier application under review, infrastructure security encompasses the following technologies:

1. The Wide Area Network including the digital satellite communications system under Frame Relay.
2. Individual Local Area Networks within departments and/or physical locations of the government running either Novell or Windows NT operating systems for the PeopleSoft application servers.
3. The Oracle database, Version 7.3.4.
4. The HP UX operating system platform for the Oracle Database Server.
5. Client workstations running a mixture of Windows 95/98 operating systems

Review Objective:

Evaluate both logical and physical security within the server operating system(s), network(s) relational database and client workstations comprising the infrastructure for the PeopleSoft application against standards established within the CICA's, 'Information Technology Guidelines' for Information Technology Security[3].

Review Procedures:

- For the above listed technologies, benchmark logical and physical security against industry best practices particular to each operating system(s), network(s) and relational database.

- Obtain an understanding of the IT infrastructure from review of network maps and discussion with management.

[3] CICA, Information Technology Control Guidelines, 3rd Edition, Chapter 6

- For a sample of decentralized locations, perform onsite review of logical and physical security over the LAN (Financial Management Board Secretariat; sample of LANs at Fort Smith) and workstations.

- For centralized database / application servers and telecommunications associated with the PeopleSoft application review logical and physical security.

- Review general information systems security policies and procedures.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
	Wide Area Network		
C.1	The communications manager has done an excellent job of documenting the WAN topology for each community. There is however, no overall topology showing the entire WAN.	We recommend an overall topology chart be created and maintained for the entire WAN. Given the number of connections and complexity of the WAN, this would be a useful high-level document to assist in security administration and management network performance. Software tools are available to assist in this process.	Low
C.2	The government is currently using a screening router as a firewall between itself and the Internet service provider, Microage. The screening router provides limited firewall type functionality.	We recommend that the Firewall architecture controlling Internet/Intranet access is improved by properly locating a Proxy Server(s) with best practices Firewall software before access points to internal networks. These improvements add filtering capability, access monitoring, intrusion alerts, and screen internal networks. These capabilities enhance intruder prevention and detection.	High
C.3	Satellite communications are used to uplink – downlink data to/from remote locations using unencrypted messaging via frame relay transmission protocol. Encrypting these messages to prevent unauthorized disclosure of information has not been implemented due to the performance burden this would impose on the system.	We recommend that the trade-off between systems performance and security be revisited from time to time as technology progresses with the view to implementing encryption techniques as soon as possible.	High

Ref#	Findings	Recommendations	Significance
	Local Area Networks		
C.4	An overall concern is that there appears to be no consistency amongst networks in terms of administration and security. Each department is solely responsible for their respective local area network. As a result, each LAN is different in terms of its configuration, security, hardware, network operating system, etc.	Network standards for hardware and operating system security settings (i.e. lockout rates, system logging, password standards, etc.) should be established and implemented. Periodic, independent reviews for compliance with these standards should be carried out.	High
C.5	We found a number of users (i.e. 20 of 167 in the FMBS network server) defined on the network operating systems examined who have not signed on for some time (i.e. prior to Jan 1, 1999). These are likely former employees whose accounts have not been removed from the system.	We recommend each LAN administrator review the network user accounts and remove former employees. Additionally, similar to Item B.2.3, we recommend the process of removing departed employees be reviewed by the management of the various departments to ensure the process is operating effectively.	High
C.6	We found several network user accounts that did not require a password and other 'guest' accounts existed on networks whose use was not linked to individuals.	All network user accounts should require a password defined using best practices for passwords and guest accounts should be disabled wherever practicable. If guest accounts are required, the access rights to the guest account should be restricted and closely monitored.	High
C.7	We did not identify any automated system activity logging being carried out on the LANs we examined. For example, Novel intrusion detection was not turned on in all containers, NT Event Viewer was not being reviewed and the Novell Auditcon utility was not being utilized.	The timely review of audit logs is an important detective control for network security. Management should address system logging to identify events of interest, assign responsibilities for this procedure, and prepare incident response plans/procedures.	High
C.8	Physical security of networks and network servers is compromised because wiring closets are not locked or otherwise secured.	Wiring closets and other locations housing telecommunication devices for networks should be physically secured.	High
C.9	The NT and Novell Administrator accounts have not been changed. The Administrator account is a potential target to system intruders because of its well-known default name and superuser capabilities.	We recommend a policy be established requiring that all 'Administrator' accounts be renamed and "decoy" Administrator accounts without permissions take their place. Access to the "decoy" accounts should be monitored for	High

Ref#	Findings	Recommendations	Significance
		intruders.	
C.10	We found certain non-PeopleSoft application files stored on network servers with file attributes set as read and write. Write attributes increases the risk that application program files are deleted.	Policies for file level security should be established and implemented.	High
	Oracle Database		
C.11	The auditing feature of Oracle has not been enabled. The creation and review of logs is an important security control over the database. Review of logs may detect whether unauthorized access to the database has been attempted and/or granted.	We recommend the logging feature of Oracle be enabled and logs reviewed by the Database Administrator or a Security Officer on a timely and periodic basis. In particular the actions of SYS, SYSTEM and DBA accounts should be independently reviewed, as they are powerful accounts.	High
C.12	Additionally, The version of Oracle in use (Version 7.3.4) lacks basic password management functionality.	To improve security over the production database, the production version of Oracle should be upgraded to Version 8, which has much improved password management functions. Meanwhile, to compensate for the lack of basic password administration functions in Oracle 7.3.4, management should consider one of the following: ▪ Enforce manual password management such as minimum password length, password expiry and password history. ▪ Use the operating system to authenticate users and thereby take advantage of the password management functionality of HP UX.	High
C.13	The Database Administrator does not use the Oracle Enterprise Manager. The Enterprise Manager is a useful tool for administering users and security on the Oracle system.	We recommend that the database administrator use Enterprise Manager when performing his database administration functions.	Medium
C.14	Other than the Database Administrator, there is no one skilled as a Oracle database administrator within the Government to replace him if he is	The Database Administrator is a key position within the PeopleSoft support group and it is	High

Ref#	Findings	Recommendations	Significance
	unavailable.	important to have someone cross-trained in database administration in case current database administrator is unavailable.	
	HP UX Operating System		
C.15	During our review of the HP UX (UNIX) operating system we noted that too many users have knowledge of the Root password. Additionally, we noted instances where a user switched to Root, effectively giving them Root level access. The Root account is the most powerful account in the UNIX environment and as such should be tightly controlled. We also noted several instances were passwords were shared for various accounts such as Oracle, Operator, Root and PSDEV	We recommend that the UNIX administrator's account for the UNIX machine be given permissions needed to perform his duties and the Root account not be used. The password for the Root account could be kept in a physically secure location within a sealed envelope. In an emergency situation requiring Root account privileges, the password can be retrieved. Passwords for user accounts should never be shared. Shared accounts cause the loss of accountability on the system. All UNIX users should have their own account with the password known only to that user.	High
C.16	Given that the UNIX server's purpose is to house the Oracle database, we expected to see very few user accounts on the operating system since the PeopleSoft application connects all users to the database using the 'psoft' account. During our review of these users, we noted 8 accounts and were informed that these accounts are used by people in the finance department to FTP into the UNIX server and transfer files used for the Financial Information System Interface. FTP functionality poses security risks since it can facilitate unauthorized files to be introduced into production systems. Lastly, full read, write and execute permissions of the 'tmp/interface/prod/fis' directory which stores the files used for FTP are available to all UNIX users.	We recommend that the access for the purpose of FTP been reduced to small group as possible. One individual should be given assess for purpose of FTP with the addition of an additional user as a back up. All other user accounts should be removed immediately. The permissions on this directory should be limited such that only designated FTP users have access to this directory. A superior solution would be to allow only outgoing FTP and have the UNIX administrator copy the necessary files into a directory accessible only by the individual from the finance department responsible for the interface.	High

Ref#	Findings	Recommendations	Significance
C.17	A standard UNIX installation creates a number of standard default accounts.	These accounts should be reviewed and, if not required, removed from the system. The fewer user accounts on the UNIX system, the lower the risk of unauthorized access and easier it is to administer.	Medium
C.18	There is currently no logging performed of the UNIX operating system. Management should decide what type of logging would be useful and have someone review the logs for unusual activity on a periodic basis.	See similar items	High
C.19	The Trivial File Transfer Protocol ("TFTP") Service is currently installed on the system. This is a high-risk service, as the use of TFTP does not require a login or password. As such, it can be used to access key system.files (such as password files) without authorization.	We recommend this service be removed as soon as possible as it is not used and it represents a serious security threat.	High
C.20	The password file is not being "shadowed". Currently, the file etc/passwd contains all of the users on the UNIX machine along with their encrypted passwords. This file is readable by all users. It is very easy for an individual to use that password file and "crack it" thereby revealing other users passwords. Cracking programs are readily available off the Internet and are easy to use.	We recommend using a shadow password file to mitigate this risk. The shadow password file, like the /etc/passwd file, is owned by the Root account. The shadow password file contains the actual encrypted password files and is readable only by the Root account. The /etc/passwd file contains a single character , usually an "x" or "!" in the encrypted password field creating a link to the shadow password file.	High
	Workstations		
C.21	During a random review of workstations, we found some with virus protection programs and others without. Computer viruses are a very real threat that can result in serious damage to programs and data.	A virus protection program should be installed on all machines as soon as possible. The application of theses programs should, if circumstances permit, include Terminate but Stay Resident (TSR) routines that continuously search the computer memory for viruses. All users should be educated on the use of virus software and the policies and procedures established to protect against viruses. A process for routinely updating the virus protection software is an important part of this type of protection (weekly updates are now becoming standard in business).	High

D. Functional Requirements and Fit Analysis

1. Legislative Compliance

Review Objective:

Determine whether data selected for the system meets user's expectations to satisfy GNWT and related agencies authorities requirements.

Review Procedures:

- For the documents listed below, on a sample basis, judgmentally select a sample (3 key items) relating to payroll and determined if the payroll and human resource system processes and reporting is in compliance.
    - Financial Administration Act and Regulations
    - Public Service Act and Regulations
    - Human Resource Manual
    - Excluded Employees' Handbook
    - Managers' Handbook
    - Northwest Territories Teachers' Association Collective Agreement
    - The Union of Northern Workers Collective Agreement
    - Affirmative Action Directive
- For each of the collective agreements, select a sample (10 pay rates) from the wage scales and ensure they are correctly input into the PeopleSoft system.
- For each of the federal payroll tax tables (CPP, EI, and Income tax) and the Northwest Territories tax tables, select a sample (5 deduction rates) and ensure they are correctly input into PeopleSoft System.

- Test that the union deduction rates are correctly programmed and that the pay base to which the rate is applied is correctly calculated.
- Test that the superannuation rate is correctly programmed and that the pay base to which the rate is applied is correctly calculated.
- Review the reporting requirements of superannuation and ensure that the PeopleSoft system produces the information needed for this reporting.
- Review the reporting requirements of the Public Service Annual Report and ensure that the PeopleSoft system produces the information needed for this reporting.
- Review how the PeopleSoft system incorporates Sealift, Honorariums, and Set-offs (student loans, property taxes, etc.)

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
D.1.1	The interface to create the extract for superannuation reporting purposes has not been completed. The PeopleSoft team is aware of this requirement and is currently working on developing a data extract that can be sent by tape to the Superannuation Administration.	None	Medium
D.1.2	We were unable to recalculate the income tax deduction for one of the five test cases we performed. This information has been passed to the PeopleSoft Implementation Team who are currently reviewing this.	Complete the investigation of a possible programming error as identified by this review	High

2. Reports required by system specifications

Review Objective:

To ensure standard PeopleSoft reports are available to users.

Review Procedures:

1. Review the Reports section of the user manual to determine if the standard PeopleSoft reports are being made available to users.
2. Review mapping documentation matching reports from the old systems with that of the PeopleSoft system.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
D.2.1	The PeopleSoft job scheduler is not being used to run reports. Reports are being submitted and tracked manually, awaiting the implementation of this feature.	Set up the job scheduler with the reports and frequency as soon as possible to cut down on manual involvement and the potential for missing a report.	Medium

3. Adequacy of System documentation

Review Objective:

To ensure that adequate system documentation exists for capturing all phases of the project.

Review Procedure:

Review the Project Team's documentation and evaluate against standard practices for PeopleSoft Implementations

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
D.3.1	Some documents have been started, but not maintained or finalized. Many of these documents will be very valuable for future projects, especially for the Nunavet installation	Finalize all deliverable documentation as soon as possible. (Particularly any documentation to be completed by consultants should be finalized before leaving this assignment.).	Medium

E. Change Control Processes

Review Objective:

Assess program change control processes against standards established within the CICA's, 'Information Technology Guidelines' for Information Technology Security[4].

Review Procedures:

1. Inquire as to program change control processes with the Functional Team leader, team members and the Public Works and Services (PWS) operational staff.
2. Review change control methodology and associated change control documentation.
3. Review tracking databases for faults and customizations.
4. Review PeopleSoft on-line change control functionality in Application Designer
5. Review modified SQR, COBOL and PeopleCode programs.
6. Review documented procedures.

Findings and Recommendation:

Ref#	Findings	Recommendations	Significance
E.1	Documentation of the modified, changed, or fixed SQR programs, Cobol and PeopleCode were accurate and thorough. Documentation included information on whom, why, when a change was applied. Code was commented on the line where the change occurred. However, we could not trace the modifications back to a specific change request.	A service request or customization number should always be used when making modifications to a program. The annotated code should reference the customization number, thereby enabling a trace of the modifications back to the change request	Medium
E.2	There are two databases used to track changes. One is used to track	Consideration should be given to merging the	Low

[4] CICA, Information Technology Control Guidelines, 3rd Edition, Control Objective M

Ref#	Findings	Recommendations	Significance
	customizations and the other is used to track fault corrections. The customization database is then used to produce customization detail reports. These reports indicate who did the change, what was changed, when it was changed or completed and the signature for approval to move to production.	two change databases into one. The would allow all program changes to be kept in one location and reduce the overhead required to maintain two separate databases	
E.3	The correction of faults does not require a signed change request.	The correction of faults should be subject to the same change control procedures as other changes. That is, the change needs to be requested, approved, and documented in the same way as customizations.	Medium
E.4	Currently, most members of the PeopleSoft implementation team have full access to the production database and PeopleCode. This includes members of the technical team, who are involved with making changes to tables and PeopleCode. This creates a risk that programmers can make unauthorized changes to production data and programs that either intentionally or accidentally damages the integrity of the PeopleSoft processing.	Direct access to the production database and PeopleCode should only be permitted to the Database Administrator or other designated person(s) who are independent of programming. As well, these persons should only have the ability to move changes into production and have no rights to make changes to the production database and PeopleCode. This can be accomplished using the Object Security Manager built into the application. Note: It is considered fundamental to the integrity of the PeopleSoft system that the COBOL code is not subject to change.	High
E.5	We note that there are no formal processes for carrying out emergency fixes of Tables or PeopleCode.	We recommend that: ▪ Criteria for determining what constitutes an emergency fix should be established, and ▪ Procedures for carrying out emergency fixes in a controlled manner should be established. (Consider, documentation, post change authorization, and automated secure logging of change event.)	High

F. Implementation Integrity

1. Data Conversion Strategy and Plan

Preamble

The conversion strategy appears to be well planned and thought through. High level outlined areas include:

1. The data sources
2. Conversion assumptions
3. Automated and manual approaches
4. Differences for Nunavut and small companies
5. Data porting procedures
6. Audit procedures
7. A conversion schedule.

Review Objective:

Evaluate the integrity and completeness of the conversion strategy and plan for data.

Review Procedures:

1. Review the GNWT Conversion Strategy document.
2. Inquire of the Project Team management the aspects of the conversion plan, procedures and results.
3. Examine documentation supporting conversion procedures, data cleanup, data mapping, data reconciliation and other documentation surrounding the activity of data conversion.

Findings and Recommendations

Ref#	Findings	Recommendations	Significance
F.1.1	The Working Committee passed a decision on November 19, 1998 not to convert any history records from GHRS into the new HRMS, due to the inability to fully clean up this data in a timely manner. The team stated that, by not converting historical records from GHRS there will be a very clean conversion to the new HRMS. This decision creates some inefficiency within the new system when retroactive pay processing may be required.	Given the importance of the historical data especially for retroactive pay processing it is important the GRHS data remain intact, stored in a secure manner and readily available if circumstances require.	Medium

2. Project Management Disciplines

Review Objective:

Determine if standard industry project management disciplines were incorporated and followed throughout the project.

Review Procedures:

1. Inquiry with the Project Management on project management practices
2. Review Project Management documentation.

Consider:

- Project tracking and reporting
- Change management and control
- Acceptance of deliverables
- Communications
- Quality Assurance
- Testing
- Documentation/Information Management
- User training and documentation

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
F.2.1	A thorough project plan (created in MS Project) was created, but has not been maintained over time. The management of the project switched from task management to deliverable management. A document was produced, "Major Changes to the Project Work Plan Version 6 → Version 7.2", on January 5, 1999. A newly created Project Work Plan was then created and used as the final Project Work Plan.	We suggest that the Project Management should have continued to track the status of the project in the original project management software as well as capturing this information in another document. Even though the decision was made to move from task management to deliverable	Low

Ref#	Findings	Recommendations	Significance
		management, it would have be helpful to continue to use the project planning software that is designed to track status in a variety ways. Such a tool can identify tasks starting late, tasks not started, significant impacts on the plan, etc.	
F.2.2	The Risk Management Plan looks like it was not prepared until March 15, 1999, a date too late to make changes in order to meet the original April 1, 1999 "go live" date.	We suggest that the Project Management should have conducted a risk management survey early on at the beginning of the project to identify all potential risks. This is usually conducted with management and key users from the different companies as well as key areas, such as Human Resources, Information Systems, Finance, Legal, etc.	Medium
F.2.3	"Change Management - A Business Process Re-Engineering" workshop was held April 18-22, 1999 for key liaison users to help them understand the various changes, to prepare them to help others in their organizations understand the changes. The slides from the workshop indicate significant material was well communicated. Given the original project 'go live' date, this workshop was not scheduled in a timely manner.	We suggest that important information in connection with major corporate changes should be delivered as early as possible and multiple times. Changes of the magnitude of this Project require multiple communications in a variety of ways.	Medium
F.2.4	Deliverables were identified, defined, and assigned. We did not receive evidence of the actual signed off deliverable documents due to the timing of our review.	Project Management should ensure signed off deliverable documents evidencing project completion are obtained as planned.	Medium
F.2.5	A Quality Assurance Plan was identified as an original deliverable, however it does not appear on the completed or outstanding deliverables log.	A Quality Assurance Plan should be included in the deliverables of the Project.	Medium
F.2.6	A Communications Plan was drafted on May 15, 1998. This document details the audience for updates on the project and potential ways of communicating, however, no specific plans with dates and deliverables were found beyond that.	We suggest that the Project Management should have created a schedule for communications with dates or date ranges, what type of communication is to be distributed and whom it is assigned to. This can then be tracked similarly to any other deliverable.	Low
F.2.7	In discussion with the Director of Computer Services and Communications, we discerned that the designated Database Administrator for this system has yet to be fully instructed in the operations and management of the application and associated Oracle database. As well, there is no indication of when and how	We stress the importance of ensuring that the designated Database Administrator is made as fully knowledgeable of the system as possible. Prudence requires that at least a second person	High

Ref#	Findings	Recommendations	Significance
	this instruction will be delivered. In this regard, we understand that the scheduled weekly meetings between the Implementation Team consulting database administrator and the designated Database Administrator did not occur.	also have the requisite skills and training (see Item C.13).	

G. Operational Controls

1. Manual, clerical, and supervisory control and management procedures

Review Objectives:

Evaluate adequacy of operational controls over the PeopleSoft system to accomplish the following control objectives:

- Segregation of Duties
- Authorization of Transactions
- Accuracy and Completeness of Data Entry
- Accuracy and Completeness of Processing
- Integrity of Data

Review Procedures:

Identify and benchmark internal controls designed into the GNWT implementation of PeopleSoft HRMS version 7.0 system against the Grant Thornton InFocus™ Controls Evaluation methodology. Consider the following business processes:

- Hiring Process
- Employment Termination Process
- Time entry (Time and Labour)
- Changes to Employee records (promotion, raise, transfer, etc)
- Payroll Payment Process
- Recording of the Payroll in the General Ledger
- Paid Leave Administration (Vacation, Sick Pay, Overtime recovered)
- Benefits Administration

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
G.1.1	For the departments reviewed by us appropriate segregation of duties had been achieved. However, members of the project team brought to our attention the fact that some departments have not achieved an appropriate segregation of duties (i.e. Resources, Wildlife and Economic Development).	Segregation of Duties is a very important internal control mechanism. To achieve segregation of duties, the same individual should not perform the two or more of the following duties/functions. ▪ Data entry for payroll ▪ Approve payroll ▪ Generate payroll ▪ Audit payroll We recognize that small departments may have difficulty in separating all of the above functions. In those instances, an independent audit/review of payroll register and action history reports becomes a critical detective control. Larger departments with many employees should have no difficulty in achieving this segregation. We recommend that given the rollout of a new system, this is a good time to direct all payroll departments to re-engineer themselves to establish satisfactory segregation of duties.	High

2. On-going maintenance of system

Review Objective:

To ensure the system and all supporting processes and controls will be adequately maintained.

Review Procedures:

1. Inquire of Project Team management.

2. Review supporting documentation.

Consider:

- Help Desk
- System Updates
- User Training
- Application Upgrades
- Post-Implementation Support

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
G.2.1	There is no process for tracking helpdesk inquiries (i.e. receipt, source, description and resolution). An automated database of helpdesk queries provides useful information including an indication of areas where training or documentation weaknesses exist.	Develop processes and tools to track and report help desk inquiries.	Medium
G.2.2	There is no formal understanding between the user community and the PeopleSoft support group of the expectations for service. Without this understanding, frustrations between departments may arise, unacceptable stop gap activity may occur, and user acceptance of new systems may be affected.	Management should consider developing a service level agreement(s) between the CSS group and the users. This will help set expectations on both sides for going forward	Medium

Ref#	Findings	Recommendations	Significance
	As well, mechanisms for the prompt detection and resolution of performance issues may not be developed.	and introduce monitoring mechanisms to ensure the system performance remains satisfactory.	
G.2.3	We noted that as yet procedures for system updates (i.e. tax tables etc.) have not been developed. We understand these are planned to be completed in August, 1999.	System acceptance should not be approved until procedures for system updates have been developed.	High
G.2.4	The manuals and training resource position for the PeopleSoft system is currently vacant. Without adequate resources the on-going maintenance of user documentation and system performance may be affected.	We recommend that resources planned for maintaining and disseminating information on the PeopleSoft system should not be left vacant for extended periods of time.	Medium
G.2.5	The data entry forms were not yet finalized at the time of our review, awaiting feedback from certain regions and departments. Final forms, complete with logos, are scheduled to be completed at the same time as the procedure manuals (for September, 1999), and all final forms will then be made available to the users. The form will be two-sided with the backside referencing all required code types and descriptions to facilitate more accurate completeness of the form. They may also be available on-line.	System acceptance should not be approved until the final forms have been approved, which should be done as soon as possible.	Medium
G.2.6	We note that a small team from the existing PeopleSoft Implementation Team will be formed when time permits to analyse the effort to upgrade to PeopleSoft Version 7.5. The first major PeopleSoft upgrade for any team, especially without consulting help, can be overwhelming and should be properly planned for.	We recommend that the Government provide ample time and resources to complete this upgrade.	Medium
G.2.7	There is no one designated to keep abreast of application developments and champion the application in the post-implementation period.	Management should consider creating a "PeopleSoft Coordinator Role". This is usually a role that is needed to stay abreast of the latest PeopleSoft changes, software releases, educational seminars, and "white papers". In addition, this role serves as communicator with other PeopleSoft clients for sharing ideas and solutions.	Medium

II. Security and Integrity of Application Interfaces

Preamble

At the time of our review, the interface to Financial Information System (FIS) was still in the testing phase. The interface itself is planned to be automated. There are two processes that must be run to create the "interface extract". One is a PeopleSoft process and the other is an external process. Both processes are linked to PeopleSoft menus and it is not possible for a user to change the configuration of the processes. Once the processes are complete, the interface extract is placed into an FTP directory on the UNIX server. The financial systems co-ordinator uses file transfer protocol (FTP) to obtain a copy of the extract. The extract is then imported into FIS, automating the posting of the payroll information to the appropriate general ledger accounts. The interface has the functionality to reverse out an import and start again of the need arises.

Upon completion of the import, the financial system co-ordinator runs a Payroll Reconciliation Summary Report. If the transfer was successful, the report will show the message "Payroll for this period is in balance". After a successful transfer of payroll data, the Payroll Reconciliation Summary Report will be forwarded to a reconciliation clerk who will prepare a manual reconciliation to show that payroll related reports in FIS and PeopleSoft Balance

Stanton Regional Hospital
At the time of our fieldwork, Stanton Regional Hospital was currently still developing their interfaces. Our understanding was that the general processes involved would mirror that of the government. Because of the different reporting requirement of the hospital and the different accounting principles (accrual accounting), and general ledger accounts, the development of the interface was quite separate from the development of the government's interface.

Northwest Territories Housing Corporation
At the time of our fieldwork, the Housing Corporation was going to manually enter the information after each payroll into their general ledger. Key totals from the PeopleSoft report are entered into a spreadsheet. The spreadsheet then creates a journal entry that gets posted into the Housing Corporations general ledger. The spreadsheet gets printed out and forms the back up for the journal entry.

Review Objective:

To assess whether application interfaces with Financial Information Systems (FIS) of GNWT, NWT Housing Corporation, and Stanton Regional Hospital provide adequate levels of security and integrity.

Review Procedures:

1. Inquire with PeopleSoft Implementation Team and User representatives regarding the following:

   - Interfaces with the government, Aurora College, and the Stanton Regional Hospital.
   - Process for creating the FIS interface extract.
   - Security of the extract.
   - Balancing procedures between PeopleSoft and the FIS.
   - Interface testing.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
II.1	As noted above, at the time of our visit the interface(s) was still in the development and testing stage. At the conclusion of the first live pay, for the FIS interface two balances on the audit report did not balance to the source reports. The PeopleSoft Implementation Team is investigating the differences.	System acceptance should not be approved until interface(s) have been fully developed, tested and approved. Issues identified during the first live pay should be addressed as soon as possible.	Medium
II.2	We also made inquiries in connection with the bank funds transfer extract developed each pay for delivering payment transactions to the financial institution. We noted from our inquiries that the extract file is not stored in a secure location. Specifically, we were informed that the extract file is stored temporarily while in transit on unsecured workstation drives before electronic transmission to the bank via SSL3 secured Internet transmission.	We recommend that the extract file for bank funds transfer is written directly to secured locations prior to transmission to the bank and thereafter archived in a secure manner.	High

I. Storage and Retention Requirements of Data

Review Objective:

To ensure that appropriate policies and procedures are in place to protect the organization's data.

Review Procedure:

Assess compliance of data storage and retention policies and procedures against standards established within the CICA's, 'Information Technology Guidelines'[5] via inquiry with the Database Administrator.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
I.1	There is currently no written policy on the data storage and retention requirements of the government.	A formal written policy/strategy for data storage and retention needs to be developed. The policy should address the following: ▪ When back-ups are to occur ▪ What is it to be backed up (Data, application files, system files) ▪ Who is responsible for performing the back-up ▪ Who is responsible to review that the back-up was done correctly ▪ What back-up media should be used ▪ Testing procedures for checking the back-up tapes including guidelines on how often the testing should be performed ▪ Naming and labeling conventions for the back-up tapes ▪ How long before data is removed from the	High

[5] CICA, Information Technology Control Guidelines, 3rd Edition, Control Objective O5

Ref#	Findings	Recommendations	Significance
		production database and archived ▪ Procedures to ensure legislative requirements for the retention of data are met	
1.2	Two logs are kept of the back-ups. A manually prepared log is kept in the computer room. An electronic log of back-ups is also produced. No one independent of operations reviews the back-up log on a periodic and timely basis to ensure that back up was performed.	Someone independent of computer operations should review the back-up log to ensure the procedure was completed and sign-off the log to evidence the review.	Low
1.3	There has been no formalized data capacity planning or analysis with respect to the PeopleSoft implementation.	The government should institute a formal capacity management function. The goals of capacity management are to: ▪ Assure that application systems are properly designed and configured to give efficient performance, ▪ Ensure sufficient computer capacity for present and future operations, and ▪ Contain the cost of computing. Computer capacity management includes performance management and capacity planning. Performance management involves analyzing the performance of a computer system to determine how resources are currently utilized and how utilization can be improved. Capacity planning assists in forecasting computer resource requirements to ensure that adequate capacity exists when needed.	Medium
1.4	There has been no testing of the back-up tape nor has a full recovery been attempted or tested.	The back-up media should be tested on a periodic basis to ensure the government would be able to perform a full restore of all data, applications, and system files in the event of a major failure. The Arctic43 machine could be used for this purpose.	Medium

J. Disaster Recovery Planning

Review Objective:

To ensure the adequacy and completeness of the disaster recover plan as it pertains to the PeopleSoft HRMS system accords with standards established by the CICA's, IT Controls Guidelines[6].

Review Procedure:

Obtain the disaster recovery plan of the government entitled " Disaster Recovery for Payroll Processing " dated May 4, 1999 and evaluate the plan against standards laid down by the CICA's IT Controls Guidelines.

Findings and Recommendations:

Ref#	Findings	Recommendations	Significance
J.1	The government currently does not have a disaster recovery/ business resumption plan for the PeopleSoft Human resource or Payroll functions. A document titled " Disaster Recovery for Payroll Processing" was prepared by the former PeopleSoft Implementation Manager. However, it was prepared to deal with the following three very specific contingencies: ▪ Complete System Failure ▪ Regional Communication Link Failure ▪ Complete System Failure for July 9, 1999 Pay This document is a stand-alone document and is not part of a larger disaster recovery/ business plan for Government. Additionally, the document lacks	We recommend that a comprehensive business resumption/disaster recovery strategy should be developed which integrates with the business resumption/disaster recovery strategy of the Government as a whole. Such a plan should address not just the information technology aspects of business resumption but also the business processes. The following points should be considered when developing a strategy: ▪ There should be a formal assignment of responsibilities and accountabilities for the business continuity planning processes ▪ Responsibilities should be formally assigned and communicated to staff ▪ Formal business continuity plans should be prepared for all critical business functions within HR and Payroll ▪ Once business recovery procedures have been established, personnel who will participate in recovery activities should be trained to perform their responsibilities	High

[6] CICA, Information Technology Control Guidelines, 3rd Edition, Chapter 7

Ref#	Findings	Recommendations	Significance
	sufficient detail to be considered effective and complete.	• Periodic testing of the plans should be performed. Follow-up of issues arising from these tests should be completed on a timely basis • Ensure that business continuity plans and arrangements include all resources necessary to support critical payroll and HR functions (e.g. office work space and technology, furniture, voice and data communications, supplies and services, and people resources • Ensure that communication procedures are in place (both internal and external) in the event of a disaster or business disruption • Periodically (e.g. at least annually), evaluate potential business threats and exposures which could have a detrimental impact on normal business operations and incorporate into the plans as appropriate • Ensure that all significant Payroll and HR processes are categorized as to their criticality and prioritized according to their need for availability • Assign maximum tolerable outage time periods to all significant HR and Payroll functions • Plan periodic (e.g. at least annual) testing of all significant components of business continuity arrangements to ensure their ongoing adequacy. • Ensure that appropriate personnel are trained in restoration procedures • Where direct periodic testing is not practical, confirm/review periodically that facilities for business continuity are in place and are functional • Ensure that off-site storage and back-up procedures are appropriate to meet the Payroll and HR's continuity strategy • Periodically test the adequacy and completeness of off-site availability of material required to resume/recover critical Payroll and HR processes. This should be done in coordination with periodic information technology recovery testing. • Ensure that personnel critical to the recovery efforts can be contacted	

MANAGEMENT RESPONSE TO GNWT PEOPLESOFT IMPLEMENTATION REVIEW: JULY, 1999

The following are management responses to the findings and recommendations contained in the GNWT People/soft Implementation Review completed in July 1999 by Grant Thornton. Responses have been provided by Systems and Communications, PW&S; LR&C, FMBS; and Corporate Services, FMBS.

Ref #	Management Response
A.1.1	The User Manual has been completed by LR&C. It must be noted that this Manual will be subject to frequent revision as the system changes. Updates are circulated as they are produced. The manual is now posted on the FMBS web site.
A.1.2	Work will be done by LR&C to make the User Manual more similar to the previous Benefits Administration Manual which contained administrative procedures and included sample forms. This work will be completed in the next 12 months.
A.1.3	LR&C has included a contact list page in the Manual.
A.1.4	LR&C is working to include transaction titles on all pages of the User Manual. This work will be completed along with work for A.1.2.
A.1.5	A section has been included in the User Manual explaining how it is to be updated and where comments by readers/users can be sent.
A.2.1	The system has been modified to prevent duplicate SIN's from being used.
A.2.2	This has been added to the work list and will be completed by September 2000.
A.2.3	Upgrading to 7.5 or 8.0 will be examined in early 2000 by HRMS Support.
A.2.4	This has been completed.
B.1.1	Updates have been completed. Documentation will continue to be reviewed regularly.
B.1.2	Documentation has been updated and is accurate
B.1.3	This has been rectified and will not be permitted in the future.
B.1.4	This has been rectified with documentation updated.
B.1.5	The need to segregate duties is recognized and roles are being examined and defined to avoid having system administrators making data entry changes. This will continue to be reviewed during the remaining implementation tasks and be completed by Spring, 2000.
B.2.1	As previously mentioned upgrading is being reviewed. Password policies are being prepared with completion by March, 2000.
B.2.2	Further Training for the PeopleSoft Security Officer will be scheduled for early to mid 00/01 fiscal year.
B.2.3	This has been rectified. Procedures are in place to ensure former staff and contractors have their access removed upon termination.
B.2.4	This has been rectified. The password is now kept in a locked box in the safe and is known by a limited number of persons. It will be

	changed on a regular basis.
C.1	It is in Corporate Service's plans to acquire and/or upgrade the network documentation package to provide the capability for higher-level views of the GNWT's wide area network (WAN).
C.2	Adequate firewall protection is required. A combination of GNWT initiatives have either been completed, or will be undertaken, to address this matter. These include a recent security audit by the RCMP's Site Evaluation & Inspection Team (SEIT), whose report is due in early January.
C.3	Performance problems are a real-time operational concern, throughout the entire WAN, so adding additional overhead in order to encrypt data will be an issue with remote users. The pros and cons will have to be weighed. It is likely not possible to address this analysis any time soon.
C.4	The GNWT is currently reviewing its IT functions with a view to developing a Government wide IT strategy that includes a move towards greater consistency.
C.5	The users on the network were reviewed shortly after meeting with the Auditors in July. The status is that some of the users were disabled and some were removed. None of these "old" users were left with access.
C.6	If guest accounts are required, access rights to the guest account should be restricted and closely monitored. This practice is in place in the Financial Management Board Secretariat.
C.7	Although audit logs are in place they are not reviewed. Novell intrusion detection has been enabled and Event Viewer is used regularly. Novell Auditcon is unused, although there are plans in place for its use in the near future.
C.8	Depending on the timing, this requirement should be included in the renovations to the building. As a short-term measure, consideration can be given to replacing the existing doors with a different style.
C.9	The recommendation to rename the administrator accounts was implemented on the Novell network during the week of November 7, 1999. The administrator accounts on the NT network were changed in late December, 1999.
C.10	In practice, file level security has been implemented. A policy to this effect will be developed by Corporate Services.
C.11	The auditing feature of Oracle is a powerful tool that should be utilized, and resulting reports carefully scrutinized. The overall DBA functionality within the GNWT is being evaluated, and will include this auditing tool. For the time being, the auditing feature has been turned on and is active.
C.12	Agreed that the increase in password management functionality of the later release of Oracle should be implemented at the earliest reasonable date. However, with the version of PeopleSoft now in production, it is not possible to bring in the new release of Oracle because the two products will not properly work together. This will be reviewed following the upgrade of PeopleSoft.

C.13	The DBA should have the most efficient and useful tools available to properly do the job. S&C does have the Oracle Enterprise Manager product, but has not yet made it part of the operational procedures.
C.14	Adequate DBA backup is vital to the success and integrity of the PeopleSoft system. A backup resource recently resigned from the GNWT, but a staffing competition was immediately initiated to replace this person. As well, the GNWT is evaluating a service called OracleExpertDBA, provided by Oracle Corporation, which provides agreed upon remote DBA services around the clock to this and any other Oracle based applications being utilized within the government.
C.15	Root passwords have been changed, and continue to be secured and changed every month or so. Only two people have access to the root password now. The root level access has been eliminated, with the appropriate permissions set up to access Root from the Administrator account.
C.16	FTP access procedures have been tightened up significantly, pending the controlled establishment of this capability from another server. The user accounts are currently required so that FMBS staff who need to transfer files using FTP can do so without signing on anonymously. Analysis is underway to determine the best way to remove or resituate any unnecessary accounts
C.17	Analysis is underway on which accounts should be removed from the server, after which removal will take place immediately.
C.18	Some levels of logging are already turned on. S&C is reviewing which of the logging functions should be switched on indefinitely to suitably address the concerns identified in the audit. Procedures will be implemented to ensure that the logs are properly reviewed and action undertaken when required.
C.19	– see response to C.16
C.20	This problem has been rectified.
C.21	All inventoried machines, including servers, in the FMBS have anti-virus protection installed. The exception is the GRYPHON server, which is being replaced.
D1.1	No response required.
D1.2	Investigation completed. This error was an isolated instance resulting from the specific individual's employment history. It has been corrected.
D2.1	Scheduler is now being used.
D3.1	The support team is working towards ensuring all documents are completed by April 1, 2000.
E.1	Customization manager database is being used to track and log each customization. A service request system and procedures is under development and this will be completed by March 31, 2000.
E.2	The two databases have been merged.
E.3	This will be implemented with E.1.
E4.	More rigorous procedures have been put into place for access to production. The roles of technical staff have been clearly defined. Code

	2000
G2.3	A process and procedures for fixes and tax updates will be developed and in place by March 31, 2000.
G2.4	The manuals and training position will likely be filled early in the 2000/2001 fiscal year. It is recognized that this is an important role on the team.
G2.5	Forms are in the final stages of approval and should be printed early in the 2000/2001 fiscal year.
G2.6	Time and resources for an upgrade to 7.5 or 8.0 will be examined and finalized following the post implementation review.
G2.7	The Manager will ensure that the team keeps abreast of the latest PeopleSoft Changes.
H1	The FIS interface and Stanton interface are complete.
H2.	This has been rectified.
I.1.	A records management committee for the LR&C Division has been established. It will review archive requirements for the HRMS within the next year. Such a policy is essential. It should be noted that, although this policy has not been formalized, that there are procedures in place to ensure backups are done daily for the appropriate files and databases, by Computer Operators, naming and labeling conventions for the backup tapes. For the foreseeable future, backups will be done on DDS tapes. We are looking for a mechanism to confirm that the material being backed up can be validated in some matter, to insure recoverability. There are no archiving criteria yet established, that S&C is aware of, nor are there legislated guidelines with regard to retention. Therefore, no data is being archived, and backup media is being retained indefinitely.
I.2	If necessary, or recommended, copies of backup logs can be forwarded to FMBS or some other place for scheduled or periodic review. The procedures in place for reviewing backup logs for PeopleSoft have always been applied to backups for all other servers and applications used in the data center.
I.3	Capacity planning should be done for all applications on all systems, PeopleSoft included. It is assumed that once the various implementation phases have been completed, that it will be possible to undertake routine application management functionality such as capacity planning.
I.4	It is vital to know that what data has been backed up is recoverable. This problem will be addressed through testing by March 31, 2000.
J.1	As mentioned previously a Business Resumption Plan for the HRMS has been established. A disaster plan for the PeopleSoft application is not in a satisfactory state. Such planning is high on the priority list of the Informatics Policy Committee.

	is now only moved into production with the Manager's approval.
E.5.	Procedures for emergency fixes will be completed in the summer of 2000.
F1.1	This is complete. GHRS data is stored in an Access database on a CD ROM. HiLine data is stored on micro-fiche..
F2.1	It is recognized that it would have been helpful to maintain and update the project plan and deliverables. However, it does not make sense to complete this now that the system is live.
F2.2	It is recognized that a Risk Management plan should have been prepared earlier. A Business Resumption Plan has been developed and is in place.
F2.3	LR&C and other FMBS management recognize the need for good communication with users. Experience has been gained on this area from the implementation, which will serve management well during future system changes. A walk through process will be developed and used for future changes.
F2.4	Deliverables were signed off as completed.
F2.5	A Quality Assurance Plan was not completed during the implementation. At this late stage it would not be efficient or effective to complete such a plan.
F2.6	A communication plan was completed very late in the project and was not as thorough as it should have been. During normal maintenance of the system newsletters are being provided to users on a regular basis. In addition updates and issues are discussed at HR manager and benefits administration meeting. Communications plans will be included in project planning for future major functional changes.
F2.7	Schedules have been worked out with FMBS that provides for the DBA to spend more time in the HRMS Support Section premises. The ongoing operational environment of the data center, which supports several technologies besides PeopleSoft and Oracle, must be given top priority whenever problems occur; the recent resignation of one of the Technical Support Staff, along with required travel for this group to apply final Y2K patches to remote servers, has unfortunately interrupted the time the DBA was to spend at FMBS. Furthermore, with the dubious potential to hire a replacement Technical Support staff member to support the environment and backup the DBA, the upcoming evaluation of Oracle's Expert DBA remote services program will have to include maintaining sufficient Technical Support expertise in the PeopleSoft application. The findings of the audit report coincide with the concerns of the GNWT in this regard.
G1.1	Segregation of duties in Departments is problematic and will continue to be raised with users in an effort to resolve this issue.
G2.1	The support team has started investigating help desk software. This will be in place by September, 2000.
G2.2	Service Level Agreements are in draft and will be finalized in Feb/March