#1076099

Indian and Northern Affairs Canada

Prepared by:

Audit and Evaluation Sector

Assisted by:

Deloitte & Touche, LLP

System under Development Audit of the First Nations and Inuit Transfer Payment System

Project 05/09

June 2007

Table of Contents

Executive Summary

Background

The First Nations and Inuit Transfer Payment System (FNITP) is designed to replace the Transfer Payment Management System. The goal of the FNITP project is to build a web-enabled transfer payment management system that will provide integrated service delivery and enhanced management tools for First Nations and Inuit communities. The system aims to provide improved accountability by introducing better financial and non-financial reporting capabilities for transfer payment recipients.

The FNITP system will assist Indian and Northern Affairs Canada (INAC) in managing funding arrangement information and applying prudent cash management practices in accordance with Treasury Board requirements.

FNITP includes functionality:

- to facilitate the front-end preparatory work to develop funding arrangements (e.g. budget allocation activities);
- to create and maintain funding arrangements; and
- to manage recipient reports through which expenditures are justified, results of activities are recorded, and the potential need for corrective action is identified (e.g. non-compliance with funding arrangement terms and conditions).

The FNITP project began in 2004 and is expected to be completed by March 2008, at a total cost of $13.3 million (including first year maintenance costs).

The first release of the system is currently in production, and, upon approval by the FNITP Project Steering Committee, will be used to create funding arrangements covering the 2007-2008 fiscal-year. The first release was meant to contain all of the functionality required for the beginning of the transfer payment cycle. The remaining functionality will be implemented in conjunction with the required management of the first 2007-2008 Funding Arrangements.

The financial significance of transfer payments processed by the department and the pivotal role to be played by the FNITP system in the monitoring and control of related transactions led the Audit and Evaluation Sector to include this System under Development audit in its Internal Audit Plan.

Timing, Objectives and Approach

A preliminary scoping exercise for this audit was conducted from April to June 2006 to facilitate the development of a detailed project work plan. Following the scoping exercise, it was determined that audit fieldwork would be covered through five overlapping streams from August to December 2006. As work was completed for each stream, a presentation of the results was made to the FNITP Steering Committee.

The audit objectives, as well as the streams followed to carry out the required fieldwork, are identified in the table below. For each of the streams, the detailed report contains a separate section presenting the audit methodology and timelines, the scope and the corresponding findings.

FNITP SUD Audit Objectives	Relevant SUD Audit Streams
Provide assurance that the system's functional and control mechanisms are compliant with the *Financial Administration Act* in any material respect (i.e. Sections 32, 33, and 34).	FNITP Application Controls
Provide assurance that the system's functional and control mechanisms support the Transfer Payment Management Control Framework.	FNITP Application Controls
Assess the extent and adequacy of internal systems and environmental controls, to ensure completeness, accuracy and authenticity of data that is processed and stored.	Data Input and Processing Controls General Computer Controls
Assess whether proper system and security architecture is developed to ensure sufficient protection for a web application.	Technical Vulnerability Analysis
Assess the project risks.	Project Management Controls
Assess and provide recommendations on how the project is being supported by various stakeholders.	Project Management Controls
Review the extent of compliance with development and management control practices.	General Computer Controls Project Management Controls

Scope

As the vast majority of the audit and review procedures were conducted before the first release of the application on December 11th, 2006, and all direct testing in the FNITP application was conducted in the test environment, the scope of this audit only covers the design of controls. No opinion is provided on whether or not controls have actually been implemented in the production environment, or whether they have been operating effectively over a period of time. These items should be addressed as part of a post-implementation review.

Audit work conducted in two of the streams (FNITP Application Controls and General Computer Controls) was intended to be assurance-based, whereas the audit work conducted for the remaining three streams was intended to be more consultative in nature. Caution should be exercised when relying on the conclusions stated in these three streams, as some of the findings may be based solely on information obtained through interviews.

Conclusions and Statements of Assurance

Statement of Assurance

Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the following opinions on general computer controls and FNITP application controls:

General Computer Controls

In our opinion, while a number of control strengths were identified during the audit, the design of general computer controls requires significant improvements in the following areas: logical security, testing, data conversion, disaster recovery and business continuity.

FNITP Application Controls

In our opinion, the design of application controls associated with:

- compliance with sections 32, 33 and 34 of the *Financial Administration Act* has areas requiring moderate management attention; and

- the Transfer Payments Directorate Management Control Framework requires significant improvements in the following areas: extent of the use of the system to automate controls versus providing tools to support manual controls outside of the system, segregation of duties, specific control weaknesses identified, and functionality not yet developed.

These opinions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed to by management. The evidence was gathered in compliance with Treasury Board policy, directives and standards on internal audit, and the procedures used meet the professional standards of the Institute of Internal Auditors.

Conclusions from the Non-Assurance Streams

Project Management Controls: In our opinion, project management controls are effective, with the exception of the lack of a "Go / No Go" decision framework at the time of the assessment.

Data Input and Processing Controls: In our opinion, the design of data input and processing controls within FNITP has areas requiring moderate management attention. Most of these issues will be resolved when recommendations made in the General Computer Controls and FNITP Application Controls streams are addressed.

Technical Vulnerability Controls: In our opinion, the design of controls to mitigate technical vulnerabilities is effective, with the exception of a few medium risks that can easily be addressed.

Management has developed a detailed action plan to address the issues raised throughout the report. In our opinion, the implementation of the proposed action plan will adequately address all identified areas for improvement and mitigate identified risks.

Recommendations

The audit includes a total of 18 recommendations intended to address the findings detailed in the audit report. Given that five broad areas of control were examined and the time available for specific corrective action prior to the system go-live is limited, the audit does not attempt to aggregate recommendations at a more general level.

General Computer Controls

Information Security - Access

1. Update access privileges in the production environment should be removed from the accounts of all FNITP project team members.

2. A review should be conducted to ensure that all access request forms are completed and that access privileges in the system reflect what has been approved as per the access request forms. Management should consider implementing a process to review access granted to users on a regular basis, to ensure ongoing appropriateness of access privileges.

3. A formal process involving Human Resources should be implemented to ensure that accounts (i.e. at the network, server, database and FNITP application levels) of employees who have been terminated, or who have changed roles and responsibilities, are revoked or modified on a timely basis.

Application System Implementation and Maintenance

4. Formal sign-offs should be obtained from the user community (or its representatives) confirming their agreement with the scope (e.g. completeness, appropriateness) of testing. In addition, for each test case (both internal FNITP Project Team test cases and user acceptance test cases), sign-offs should be obtained confirming that the test cases were used and that results were as expected.

5. All data cleansing activities should be approved by user management or the project sponsor. User management or the project sponsor should also approve the results of testing conducted to confirm the accuracy of cleansing activities.

6. The scope and results of data reconciliation activities should be documented as part of the "Go / No Go" checklist, to be approved by the FNITP steering committee.

Network and Systems Software Support

7. The change advisory board should ensure that requirements from the change management guide are fully implemented, specifically with regards to the requirement to provide documented test plans and documented test results.

Business Continuity Planning and Backups

8. The INAC Business Continuity and Disaster Recovery Plans should be updated to include FNITP. Processes should be implemented to ensure that both plans are tested and updated on a regular basis.

FNITP Application Controls

9. The functionality provided by FNITP should be leveraged to automate controls that support the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) to the fullest extent possible. The options to override or circumvent funding arrangement formulas, to delegate authorities, to create more than one funding arrangement per recipient per fiscal period, and to create funding arrangements without using models that have been approved by Transfer Payments Directorate should be removed. Furthermore, arrangement models should be pre-populated with signature blocks that are in-line with the requirements from the relevant authorities and policies. Alternatively, manual monitoring controls should be developed and implemented to ensure that control requirements from the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) are adhered to.

10. Manual controls should be developed and implemented for all Transfer Payments Directorate Management Control Framework control requirements that are not completely addressed by FNITP automated controls.

11. Considering the difficulties in trying to create FNITP user access profiles that match position titles, a segregation of duties conflict matrix should be developed to clearly document activities that need to be segregated. If conflicting responsibilities need to be given to specific users, monitoring controls should be implemented.

12. Users should not be given the opportunity to modify FNITP variables that can create discrepancies between data in FNITP and the hard copy funding arrangements. In addition, as long as funding arrangements are in a status where they can be modified in FNITP, the printed arrangements produced by the system should be clearly marked as draft.

13. Exception reports should be developed and used to monitor control overrides. Furthermore, FNITP should force users to provide comments when overriding mandatory reporting requirements.

14. The design of the FNITP application controls within the modules or functions that have not yet been developed should be assessed once the remaining functionality and controls are implemented, and before they are available for use.

Project Management Controls

15. A “Go/No Go” decision framework should be developed and approved by the FNITP Steering Committee. The decision framework should be used to assess the project’s readiness for the planned go-live date.

16. Knowledge transfer activities should be implemented within the project team to minimize dependencies on the project manager. Increased delegation should be a priority.

Data Input and Processing Controls

17. Until the reconciliation module is developed and implemented, reports from FNITP and the financial system should be compared on a regular basis to ensure that there are no discrepancies. The reports should be retained for audit trail purposes.

Technical Vulnerability Controls

18. The department should formally sign off on its acceptance of some of the risks identified in the FNITP Threat and Risk Assessment report, acknowledging its awareness of identified residual risks.

Section 1 - Introduction

Background

Indian and Northern Affairs Canada (INAC) has primary, but not exclusive, responsibility for meeting the federal government's constitutional, treaty, political and legal responsibilities to First Nations, Inuit, Métis and Northerners. INAC is currently responsible for the disbursement and monitoring of approximately $5.6 billion in annual Grants and Contributions. Transfer payments (Grants and Contributions) are made to First Nations, Inuit, Métis and Northerners and their organizations to enable the delivery of services to their respective community members, in accordance with Treasury Board's Policy on Transfer Payments, and are monitored in accordance with INAC's internal accountability, performance reporting and evaluation requirements.
The Transfer Payment Management System is the financial system currently used to manage the $5.6 billion entrusted to INAC for the handling of grants, contributions and other transfer payments. Most of these payments are transferred directly to about 2,000 recipients, the majority of whom are First Nations and their organizations.

The First Nations and Inuit Transfer Payment System (FNITP) is designed to replace the Transfer Payment Management System. The goal of the FNITP project is to build a web-enabled transfer payment management system that will provide integrated service delivery and enhanced management tools for First Nations and Inuit communities. The system will also improve accountability by providing better financial and non-financial reporting capabilities for transfer payment recipients. The new FNITP system will assist INAC in managing funding arrangement information and applying prudent cash management practices in accordance with Treasury Board requirements.

FNITP includes functionality to facilitate the preparation of funding arrangements (e.g. budget allocation activities), to create and maintain funding arrangements, and to manage the recipient reports which are the basis for expenditure justification, reporting on results of activities, and identification of needs for intervention.

The FNITP project began in 2004 and is expected to be completed by March 2008, at a total cost of $13.3 million (including first year maintenance costs). The first release of the system is currently in production and, upon approval from the FNITP Project Steering Committee, will be used to begin creating 2007-2008 Funding Arrangements. The first release was meant to contain all of the functionality required at the beginning of the transfer payment cycle. The remaining functionality will be implemented in conjunction with the required management of the first 2007-2008 Funding Arrangements. The financial significance of transfer payments processed by the department and the pivotal role to be played by the FNITP system in the monitoring and control of related transactions led the Audit and Evaluation Sector to include this System under Development audit in its Internal Audit Plan.

Timing, Objectives and Approach

A preliminary scoping exercise for the FNITP System under Development audit project was conducted from April to June 2006 to facilitate the development of a detailed project work plan for the audit.

The audit objectives as well as the streams followed to carry out the required fieldwork are identified in the table below. For each of the streams, a separate section of this report details the audit methodology and timelines, the scope, and the findings.

FNITP SUD Audit Objectives	Relevant SUD Audit Streams
Provide assurance that the system's functional and control mechanisms are compliant with the *Financial Administration Act* in any material respect (i.e. Section 32, 33, and 34).	FNITP Application Controls
Provide assurance that the system's functional and control mechanisms support the Transfer Payment Management Control Framework.	FNITP Application Controls
Assess the extent and adequacy of internal systems and environmental controls, to ensure completeness, accuracy and authenticity of data that is processed and stored.	Data Input and Processing Controls General Computer Controls
Assess whether proper system and security architecture is developed to ensure sufficient protection for a web application	Technical Vulnerability Analysis
Assess the project risks	Project Management Controls
Assess and provide recommendations on how the project is being supported by various project stakeholders	Project Management Controls
Review the extent of compliance with development and management control practices	General Computer Controls Project Management Controls

The purpose of pursuing each stream of audit work was:

- **General Computer Controls**: to provide assurance over the design of General Computer Controls supporting FNITP. General Computer Controls are controls related to the processing of information within the computer environment;

- **FNITP Application Controls**: to provide assurance over the design of the control activities supported by the FNITP system that are included in the Transfer Payments Directorate Management Control Framework. This includes, for example, FNITP functionalities that are being developed to support the requirements of sections 32, 33 and 34 of the *Financial Administration Act* and designed to prevent material financial misstatements;

- **Project Management Controls**: to comment on the adequacy of project management controls;

- **Data Input and Processing Controls:** to comment on the adequacy of data input and processing controls; and

- **Technical Vulnerability Analysis**: to complement the threat and risk assessment that INAC recently performed on the FNITP system with a technical vulnerability analysis of the FNITP Web-based design.

Scope

As the vast majority of the audit and review procedures were conducted before the first release of the application on December 11, 2006, and all direct testing in the FNITP application was conducted in the test environment, the scope of this audit only covers the design of controls. No opinion is provided on whether or not controls have actually been implemented in the production environment, or whether they have been operating effectively over a period of time. These items should be addressed as part of a post-implementation review.

For the assurance-based streams, information gathered during interviews was corroborated by the examination of supporting documentation and or observation. In the case of the consultative-based streams, although corroboration was conducted in certain areas, some of the findings may be based solely on information obtained through interviews.

Section 2 - General Computer Controls Assessment

Methodology

This assessment was performed using a risk-based approach aligned with the COBIT IT control framework issued by the IT Governance Institute. The methodology consisted of conducting the following audit activities for each control area included in the scope of the review:

- identify relevant control objectives for each review area;
- identify relevant control activities that completely fulfill the control objectives; and
- evaluate the design of the identified control activities (prior to go-live).

Scope and Timelines

Scope

The control areas included in this review are summarized in the table below.

Control Area	Description
Information Systems Operations	Supervising and maintaining computer systems operations. Scheduling, monitoring, and securing computer operations.
Information security	Designing, implementing, and maintaining information security, including both physical and logical security over all access paths to programs and data.
Application Systems Implementation and Maintenance	Developing, implementing (including data conversion activities), and maintaining application systems.
Database Implementation and Support	Managing the data architecture and maintaining the database management system.
Network Support	Designing, installing, and operating networks and communication software.
Systems Software	Implementing and maintaining necessary systems software, including the parameters that configure and control such software.
Business Continuity Planning and Backups	Developing an entity-wide plan to maintain and/or restore business operations, in the event of a disaster, at a level and within a time frame that is acceptable to management.

Timing

The General Computer Control assessment was conducted from June to December 2006.

Conclusion

While a number of control strengths were identified during the audit, in our opinion, the design of general computer controls requires significant improvements.

Strengths

Some of the strengths noted in this area include:

- FNITP is equipped with effective functionality to monitor system components and errors;
- strong password rules are enforced both at the network and application level;
- a ticket tracking system is used to manage both system development and changes to the application;
- a change advisory board exists to ensure that risks related to changes to INAC's Information Technology production environment are adequately assessed; and
- FNITP backups are conducted and stored in a separate building and city from where the FNITP production servers are located.

Findings and Recommendations

#	Finding	Risk	Recommendation
Information Security			
1	At the time of testing (during the week of December 11 to 15, 2006), several members of the FNITP project team had active accounts in the FNITP production environment with update access privileges to some of the system's functionality.	There is an increased risk that errors in the application may occur as a result of unintentional or intentional changes, which could ultimately affect the accuracy of data processing.	Update access privileges in the production environment should be removed from the accounts of all FNITP project team members.

#	Finding	Risk	Recommendation
2	We noted that some access request forms relating to active FNITP accounts have not been approved and that some users have access to more profiles in the system than what is documented on the access request forms. In addition, a process has not yet been implemented to review FNITP access privileges on a regular basis.	Discrepancies between authorized access privileges and actual access privileges increase the risk of inappropriate user access, thereby putting the integrity of corporate information at risk.	A review should be conducted to ensure that all access request forms are completed and that access privileges in the system reflect what has been approved as per the access request forms. Management should consider implementing a process to review access granted to users on a regular basis, to ensure ongoing appropriateness of access privileges.
3	There is no formal process in place to ensure that the FNITP access privileges of employees who have been terminated, or who have changed responsibilities, are revoked or modified on a timely basis.	There is a risk that former employees may inappropriately access the system by using access privileges that should have been cancelled.	A formal process involving Human Resources should be implemented to ensure that accounts (i.e. at the network, server, database and FNITP application levels) of employees who have been terminated, or who have changed roles and responsibilities, are revoked or modified on a timely basis.

#	Finding	Risk	Recommendation
Application Systems Implementation and Maintenance			
4	The scope of the test cases (i.e. completeness, appropriateness, etc.) has not been approved by users. Furthermore, test results and sign-offs (both within the FNITP project team and user community) have not been formally documented. This is particularly critical since several bugs were identified in the system during the testing conducted for the purposes of this audit.	If the scope of testing is not approved by users and test plans and test results are not formally documented, there is an increased risk that system functionality will be insufficient to meet needs.	Formal sign-offs should be obtained from the user community (or its representatives) confirming their agreement with the scope (e.g. completeness, appropriateness) of testing. In addition, for each test case (both internal FNITP project team test cases and user acceptance test cases), sign-offs should be obtained confirming that the test cases were used and that results were as expected.
5	There is no formal involvement from the user community or project sponsor (the director, Transfer Payments Directorate) in data cleansing activities.	There is an increased risk that inappropriate changes may be made to the master data during cleansing activities.	All data cleansing activities should be approved by user management or the project sponsor. User management or the project sponsor should also approve the results of testing conducted to confirm the accuracy of cleansing activities.

#	Finding	Risk	Recommendation
6	The project sponsor has not formally approved the results of the conversion of data (e.g. balancing and reconciliation activities).	There is an increased risk that the projects sponsor may be unaware of errors or other issues encountered during the conversion process.	The scope and results of data reconciliation activities should be documented as part of the “Go / No Go” checklist, to be approved by the FNITP steering committee.
Network and Systems Software Support			
7	Our review of a change to the operating system and the network revealed that test plans and results were not formally documented.	There is an increased risk that system functionality will not meet needs as a result of newly implemented changes to the FNITP infrastructure.	The change advisory board should ensure that requirements from the change management guide are fully implemented, specifically with regards to the requirement to provide documented test plans and documented test results.
Business Continuity Planning and Backups			
8	FNITP is not currently included in the INAC Business Continuity Plan and supporting Disaster Recovery Plan. Both plans are currently out of date and have not been tested recently.	There is an increased risk that FNITP may not meet the availability requirements noted in the FNITP threat and risk assessment.	The INAC Business Continuity and Disaster Recovery Plans should be updated to include FNITP. Processes should be implemented to ensure that both plans are tested and updated on a regular basis.

Section 3 - FNITP Application Controls Assessment

Methodology

The objective of this stream was to determine whether the design of the application controls within FNITP adequately supports the control requirements from the Transfer Payments Directorate Management Control Framework and Sections 32, 33 and 34 of the *Financial Administration Act*. The following audit activities were conducted to achieve this objective:

- control statements were extracted from the Transfer Payments Directorate Management Control Framework and Sections 32, 33 and 34 of the FAA to create audit criteria;

- the resulting audit criteria were validated with the FNITP project sponsor;

- planned FNITP application controls that address the requirements of the audit criteria were identified; this resulted in the list of FNITP controls supporting the Transfer Payments Directorate Management Control Framework and Sections 32, 33 and 34 of the FAA, and formed the scope for this stream;

- interviews were held to understand how the identified application controls will be implemented in FNITP, and what steps will be taken to ensure that those controls are working properly prior to go-live (e.g. testing activities); and

- the design of the identified FNITP application controls was documented and tested.

Scope and Timelines

Scope

The design of the FNITP application controls supporting the control framework for the Transfer Payments Directorate Management Control Framework and Sections 32, 33 and 34 of the *Financial Administration Act* defined the scope for this stream. Controls were assessed in the following areas:

- Entry Criteria / Management Assessment;
- Funding Arrangement Terms and Conditions;
- Financial and Program Reporting;
- Active Monitoring;
- Intervention; and
- *Financial Administration Act* Sections 32, 33 and 34.

Timing

The assessment of FNITP application controls was conducted from June to December 2006.

Conclusion

In our opinion, the design of application controls within FNITP related to *Financial Administration Act* requirements from Sections 32, 33 and 34 has moderate issues requiring management focus.

While a number of control strengths were identified during the audit, in our opinion, the design of application controls within FNITP related to the Transfer Payments Directorate Management Control Framework requires significant improvements. Numerous manual controls are still required to complement controls within FNITP and ensure control objectives are met.

Strengths

Some of the strengths noted in this area include:

- FNITP provides tools to manage reporting requirements more efficiently, including the automatic inclusion of mandatory reporting requirements during the funding arrangement preparation process;
- FNITP interfaces with the financial system to ensure that funding obligations and payments are only processed if sufficient funds are available; and
- security controls prevent the same user from conducting *Financial Administration Act* Section 33 and Section 34 sign-offs.

Findings and Recommendations

#	Finding	Risk	Recommendation
FNITP will not be leveraging technology to the fullest extent possible to automate controls			
1	Although funding arrangement formulas will be embedded within FNITP to ensure that funding allocations are correctly calculated, users will also be able to circumvent this control by importing allocations from a spreadsheet.	There is an increased risk that allocations within funding arrangements may not be in line with applicable policies and procedures.	The functionality provided by FNITP should be leveraged to automate controls that support the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) to the fullest extent possible. The options to override or circumvent funding arrangement formulas, to delegate authorities, to create more than one funding arrangement per recipient per fiscal period, and to create funding arrangements without using models that have been approved by Transfer Payments Directorate should be removed.
2	A user association function allows users to delegate authority in the system, which means that the key control now becomes a manual control outside of the system (e.g. how a budget officer communicates approval to the administrative assistant).	There is an increased risk that transactions and approvals may not be conducted by users who are authorized to conduct those activities, which places complete reliance on manual control outside of the system.	

#	Finding	Risk	Recommendation
3	FNITP allows the user to create more than one funding arrangement per recipient per fiscal year.	There is an increased risk of errors, and overall tracking for the recipient becomes more difficult.	Arrangement models should be pre-populated with signature blocks that are in-line with the requirements from the relevant authorities and policies. Alternatively, manual monitoring controls should be developed and implemented to ensure that control requirements from the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) are adhered to.
4	For funding arrangement models and templates: • a user can create a funding arrangement without using a model that was approved by the Transfer Payments Directorate; • regional users are able to publish amendment, budget adjustment and cash flow templates without approval from the Transfer Payments Directorate; and • signature blocks are not controlled by FNITP arrangement models to ensure that the appropriate individuals are required to sign-off either electronically or in hard copy on the funding arrangements.	There is an increased risk that funding arrangements and other key documents (e.g. notice of budget adjustments, funding arrangement amendments) may not be in line with applicable policies and procedures.	Arrangement models should be pre-populated with signature blocks that are in-line with the requirements from the relevant authorities and policies. Alternatively, manual monitoring controls should be developed and implemented to ensure that control requirements from the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) are adhered to.

#	Finding	Risk	Recommendation
Manual controls to complement FNITP automated controls			
5	Many control statements from the Transfer Payments Directorate Management Control Framework are not fully supported by FNITP application controls.	Without proper manual controls to complement the application controls built into FNITP, there is an increased risk that control requirements from the Transfer Payments Directorate Management Control Framework and *Financial Administration Act* Sections 32, 33 and 34 will not be met.	Manual controls should be developed and implemented for all Transfer Payments Directorate Management Control Framework control requirements that are not completely addressed by FNITP automated controls.
Segregation of duties			
6	The approach to security in FNITP is not based on job positions (i.e. there is no one-to-one mapping of FNITP security profiles to position titles) and no segregation of duties analysis tools have been developed to ensure that conflicting responsibilities are not given to users.	There is an increased risk of introducing segregation of duties conflicts.	Considering the difficulties in trying to create FNITP user access profiles that match position titles, a segregation of duties conflict matrix should be developed to clearly document activities that need to be segregated. If conflicting responsibilities need to be given to specific users, monitoring controls should be implemented.

#	Finding	Risk	Recommendation
FNITP application control weaknesses noted			
7	Users can modify the value of key data to be included on the hard copies of funding arrangements, which can lead to the hard copy of the funding arrangement being different than the copy stored in FNITP. This is also the case for notices of budget amendments and amendments to existing funding arrangements. Also, users can print a funding arrangement in its final format when the funding arrangement can still be modified in FNITP.	There is an increased risk that the hard copies of funding arrangements, which are officially signed for contractual purposes, may differ from the funding arrangements in FNITP, which are used to trigger payments.	Users should not be given the opportunity to modify FNITP variables that can create discrepancies between data in FNITP and the hard copy funding arrangements. In addition, as long as funding arrangements are in a status where they can be modified in FNITP, the printed arrangements produced by the system should be clearly marked as draft.
8	Exception reports have not been developed to monitor control overrides. In addition, users can override a mandatory reporting requirement without submitting an explanation.	There is an increased risk that reporting requirements are not in-line with management's expectations.	Exception reports should be developed and used to monitor control overrides. Furthermore, FNITP should force users to provide comments when overriding mandatory reporting requirements.

#	Finding	Risk	Recommendation
Functionality not included in the December 11th, 2006 release of FNITP			
9	Some FNITP functionality and related application controls were not included in the first release of FNITP implemented on December 11, 2006. This includes: • recipient reports management workflow for First Nation audited financial statements; • intervention module; • payable after year-end payment transactions; • FNITP – OASIS reconciliation module; and • report functionality to support monitoring of INAC's status regarding its performance standards (i.e. reviewing monthly reports within 30 days, quarterly reports within 45 days, etc.)	This impacts the scope of the current audit (e.g. controls within the modules that have not yet been developed have not been assessed).	The design of the FNITP application controls within the modules or functions that have not yet been developed should be assessed once the remaining functionality and controls are implemented, and before they are available for use.

Section 4 - Project Management Controls Assessment

Methodology

Our assessment was based primarily on the conduct of documentation reviews and interviews with key project stakeholders within INAC. Numerous meetings were held with the First Nations and Inuit Transfer Payment System (FNITP) project manager, project stakeholders from INAC headquarters (i.e. the Director of Administration Services, a representative of the Information Management Branch's Project Management Office, the FNITP project sponsor), and three FNITP regional coordinators (i.e. Quebec, Saskatchewan and Nunavut regions). Our assessment was based on a comparison of current practices against best practices for large IT system implementation projects.

Scope and Timelines

Scope

The assessment of project management controls focused on seven key areas, as follows:

Control Area	Description
Organization	The organizational structure, roles and responsibilities for the FNITP project are well defined and appropriate.
Work Planning and Scheduling	Project planning documentation is available, appropriately communicated and details how the project will be executed and monitored.
Issue Management Process	The issue management process ensures that issues related to project activities are documented, communicated, and resolved in a timely manner.
Risk Management	The risk management process ensures that project risks are managed proactively and according to a pre-determined process.
Scope Management	A scope management process is in place to ensure that the project includes all required steps and that changes to the scope during the project are managed.
Communications and Reporting	Communications and reporting regarding expectations, progress and status of the overall project is consistent, effective and provided on a timely basis.

Control Area	Description
Quality Management	The quality management process ensures that the project satisfies the needs for which it was undertaken.

The project management controls assessment was consultative in nature, and as such, some findings may be based solely on information gathered through interviews.

Timing

The assessment was conducted from July to October 2006. The project management controls assessment report was originally submitted on October 31, 2006.

Conclusion

In our opinion, project management controls are well established, with the exception of the lack of a "Go / No Go" decision framework at the time of the assessment.

Strengths

Some of the strengths noted in this area include:

- a steering committee that has been in place from the very beginning of the project;

- stakeholders that believe that they were appropriately consulted during the scope definition phase and that no major scope changes have taken place;

- FNITP regional coordinators in each region that can facilitate communications between First Nations, INAC regional staff and the FNITP project team; and

- documented standards and guidelines that have been developed by the FNITP project team for the development of the application, for change management, and for quality assurance.

It is recognized that, as the audit assessment was conducted close to the initial go-live date, the likelihood of occurrence of the identified risks is somewhat reduced. Considering, however, that the FNITP project team's mandate extends until March 2008, our observations may serve as lessons learned to be taken into account when planning future developments within the FNITP initiative.

Findings and Recommendations

#	Finding	Risk	Recommendation
1	Some of the key project deliverables, including many of the test cases, had not yet been completed when the project go-live date was less than two and a half months away.	There is a risk that the application will not have the desired degree of accuracy and completeness at the planned go-live date.	A "Go / No Go" decision framework should be developed and approved by the FNITP steering committee. The decision framework should be used to assess the project's readiness for the planned go-live date.
2	The project manager's responsibilities are numerous and of significant importance to the successful completion of the project.	In the event that the FNITP project manager would no longer be available, there is an increased risk that the timely completion of the project could be jeopardized.	Knowledge transfer activities should be implemented within the project team to minimize dependencies on the project manager. Increased delegation should be a priority.

Section 5 - Data Input and Processing Controls Assessment

Methodology

The objective of this stream was to determine whether data input and processing controls embedded in FNITP are in line with best control practices. A subset of the recommended application control objectives from the CobiT 4.0 framework were used for the review. CobiT is an IT governance framework and supporting toolset published by the IT Governance Institute. The following audit activities were conducted:

- identify relevant control objectives for each category;
- identify relevant application controls that fulfill the control objectives; and
- evaluate the design of the identified application controls (prior to go-live).

Scope and Timelines

Scope

The following control areas and objectives from CobiT 4.0 were assessed:

Control Area	Description (Objective Names from CobiT 4.0)
Data Input Controls	AC6 Data Input Authorization Procedures
	AC7 Accuracy, Completeness and Authorization Checks
	AC8 Data Input Error Handling
Data Processing Controls	AC9 Data Processing Integrity
	AC10 Data Processing Validation and Editing
	AC11 Data Processing Error Handling
Boundary Controls	AC17 Authenticity and Integrity
	AC18 Protection of Sensitive Information During Transmission and Transport

The data input and processing controls assessment was consultative-based, and as such some findings may be based solely on information gathered through interviews.

Timing

The assessment of data input and processing controls was conducted from June to December 2006.

Conclusion

In our opinion, the design of data input and processing controls within FNITP has moderate issues requiring management focus.

Strengths

Some of the strengths noted in this area include:

- edits checks are used to control the quality of data inputs and produce error messages when issues are identified. Transactions are not processed unless users address error messages;
- transactions generate detailed audit trails; and
- reports submitted by recipients are only considered final after the reports have been reviewed by INAC personnel for appropriateness.

Findings and Recommendations

#	Finding	Risk	Recommendation
Data Input Controls			
1	The reconciliation module that will compare funds committed according to the financial system with funds committed according to FNITP has not yet been developed, and is not planned to be implemented before March 2008.	There is an increased risk that discrepancies between FNITP and data in the financial system may not be detected on a timely basis.	Until the reconciliation module is developed and implemented, reports from FNITP and the financial system should be compared on a regular basis to ensure that there are no discrepancies. The reports should be retained for audit trail purposes.

Section 6 - Technical Vulnerability Analysis

Methodology

The analysis included both network and application-level vulnerability assessments. The network vulnerability assessment methodology was designed to detect weaknesses in network services and to minimize the risk during testing of denial of service or data corruption. This methodology included host profiling, as well as service profiling and vulnerability identification. The application-level vulnerability assessment testing was performed under two scenarios: 1) against the application by an anonymous hacker without an account and 2) against the application by a user with a valid application account.

Scope and Timelines

Scope

The following items were in scope: a network vulnerability assessment, an application vulnerability assessment, and an update on the status of the action plan to address recommendations from the FNITP threat and risk assessment report.

The following items were not in scope: a complete examination of the underlying network infrastructure and the Corporate Application Security Controller module used to support the FNITP login.

The technical vulnerability assessment was consultative in nature and, as such, some findings may be based solely on information gathered through interviews.

Timing

The Technical Vulnerability Assessment was conducted from November 8 to November 14, 2006.

Conclusion

In our opinion, the design of controls to mitigate technical vulnerabilities is effective, with the exception of the medium risks detailed below. These risks can be easily mitigated by implementing the suggested recommendations.

Strengths

Some of the strengths noted in this area include:

- a Threat and Risk Assessment and Statement of Sensitivity were recently conducted on the FNITP system;
- Secure Socket Layer encryption is used by the application to secure communication between the web server and the web browser clients; and
- a virtual private network offers additional protection for users who are accessing FNITP from outside of the INAC network (e.g. First Nations users).

Findings and Recommendations

#	Finding	Risk	Recommendation
Status of the Threat and Risk Assessment Recommendations Action Plan			
1	According to the action plan, several risks, noted in the FNITP threat and risk assessment, have been accepted. However, the department has not officially signed-off on the acceptance of these risks or created an action plan to address them.	There is an increased risk that senior management is not aware of the residual risks from not addressing all of the threat and risk assessment recommendations prior to the system go-live date.	The department should formally sign off on its acceptance of some of the risks identified in the FNITP threat and risk assessment report, acknowledging its awareness of identified residual risks.
2	For two of the threat and risk assessment recommendations, a decision as to whether or not to address the recommendation has not yet been made, and is not planned to be made before March 31, 2007, when the FNITP application will already be in production.		
3	For two of the threat and risk assessment recommendations, although an action plan to address the recommendations has been agreed to, the action plan won't be implemented until the next fiscal year, when the system will already be in production.		

Action Plan

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System** **Project: 05/09**
Region or Sector: **Chief Financial Officer Sector** **Page: 1 of 9**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
General Computer Controls 1. Update access privileges in the production environment should be removed from the accounts of all FNITP (First Nations and Inuit Transfer Payment) project team members.	• As FNITP project team members do not have RCMs associated with them, they cannot carry out any financial transaction or effect changes to existing financial data. • as part of their roles and responsibilities, FNITP helpdesk members have the privilege to create new users or modify system tables. The helpdesk will be transitioned to the Transfer Payments Directorate in October 2007. • In the meantime, access will be monitored on a periodic basis (monthly) and all access (read access) will be removed from the project team at the end of the project. • Finally, the Information Systems Directorate is proposing to control all INAC application accounts centrally by March 2008.	FNITP Project Director	October 31, 2007 March 31, 2008
2. A review should be conducted to ensure that all access request forms are completed and that access privileges in the system reflect what has been approved as per the access request forms. Management should consider implementing a process to review access granted to users on a regular basis, to ensure ongoing appropriateness of access privileges.	The adequacy and completeness of access request forms as well as access privileges granted will be verified in future compliance activities to be carried out by the Compliance Unit of Transfer Payments Directorate starting in fiscal-year 2007-2008 and subject to an annual risk assessment.	Transfer Payment Director	March 31, 2008

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System** **Project: 05/09**
Region or Sector: **Chief Financial Officer Sector**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
3. A formal process involving Human Resources should be implemented to ensure that accounts (i.e. at the network, server, database and FNITP application levels) of employees who have been terminated, or who have changed roles and responsibilities, are revoked or modified on a timely basis.	A procedure, including a checklist, was developed by the Information Management Directorate to ensure that the FNITP access granted to employees leaving the department is revoked. Starting in fiscal-year 2007-2008, the effectiveness of this control will be assessed in future compliance activities which will be carried out by the Compliance Unit of Transfer Payments Directorate.	Transfer Payment Director	March 31, 2007 Complete March 31, 2008
4. Formal sign-offs should be obtained from the user community (or its representatives) confirming their agreement with the scope (e.g. completeness, appropriateness) of testing. In addition, for each test case (both internal FNITP Project Team test cases and user acceptance test cases), sign-offs should be obtained confirming that the test cases were used and that results were as expected.	Subsequent to this recommendation, FNITP completed a very rigid testing initiative to obtain formal sign offs for each script scenario performed. These scripts are the most critical aspect of FNITP (i.e Section 32, Section 34, Section 33 and their respective interface with OASIS). Furthermore, users are using the system in production, which enables them to provide feedback on areas for improvement.	FNITP Project Director	February 28, 2007 (Implemented)
5. All data cleansing activities should be approved by user management or the project sponsor. User management or the project sponsor should also approve the results of testing conducted to confirm the accuracy of cleansing activities.	The project sponsor has reviewed and approved the data conversion document, including the data cleansing activities and the results of testing.	Transfer Payment Director	January 31, 2007 (Implemented)
6. The scope and results of data reconciliation activities should be documented as part of the "Go / No Go" checklist, to be approved by the FNITP steering committee.	The project steering committee approved the data reconciliation activities through the "Go / No Go" checklist.	FNITP Project Director	January 31, 2007 (Implemented)

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System** **Project: 05/09**
Region or Sector: **Chief Financial Officer Sector** **Page: 3 of 9**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
7. The change advisory board should ensure that requirements from the change management guide are fully implemented, specifically with regards to the requirement to provide documented test plans and documented test results.	The change advisory board process is currently under review. IMB will ensure that the risk is addressed through the documentation of test plans and test results in terms of changes to the server/computer and network infrastructure.	Chief Information Officer	December 31, 2007
8. The INAC Business Continuity and Disaster Recovery Plans should be updated to include FNITP. Processes should be implemented to ensure that both plans are tested and updated on a regular basis.	As part of the Management Information Technology Security (MITS) action plan, the department has created an updated Informatics Disaster Recovery Plan for FNITP as a mission critical system.	Chief Information Officer	January 31, 2007 (Implemented)
FNITP Application Controls 9. The functionality provided by FNITP should be leveraged to automate controls that support the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) to the fullest extent possible. The options to override or circumvent Funding Arrangement formulas, to delegate authorities, to create more than one Funding Arrangement per recipient per fiscal period, and to create Funding Arrangements without using models that have been approved by Transfer Payments Directorate should be removed.	The FNITP steering committee acknowledges the risk given the current INAC regional funding methodology and business process change management strategies. Although FNITP, possessing controls and system security similar to OASIS, provides the ability to reflect the application of the FAA Sections 32, 33, and 34 activities, it cannot recognize the approval of these activities as an official electronic approval and still requires a formal signature. Therefore, the risk exists that there could be a discrepancy between what is electronically recorded and what has been manually signed.		March 31, 2008

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System** **Project: 05/09**

Region or Sector: **Chief Financial Officer Sector**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
Recommendation 9 - (Continued) Furthermore, arrangement models should be pre-populated with signature blocks that are in-line with the requirements from the relevant authorities and policies. Alternatively, manual monitoring controls should be developed and implemented to ensure that control requirements from the Transfer Payments Directorate Management Control Framework and the *Financial Administration Act* (Sections 32, 33 and 34) are adhered to.	To provide assurance that FNITP reflects the signed decisions of RCMs and financial officers, monitoring will occur to compare the manually signed documents to the electronically recorded amounts. This monitoring will be performed throughout the year by the TPD Compliance Unit who will perform sampling in each region subject to an annual risk assessment. To mitigate the risk and facilitate the monitoring, the FNITP Project will implement the following:	Transfer Payment Director	March 31, 2008
	• formal Section 32, Section 33 and Section 34 reports have been developed within FNITP to reflect what has been recorded in FNITP. These FNITP reports represent the FAA documents that RCMs and financial officers should sign, hence ensuring that what is in FNITP reflects what has been signed; and	Transfer Payment Director	June 30, 2007
	• the signed Sections 32, 33, 34 documents will also be scanned into CIDM (INAC's document management tool) as official documents and information from these documents recorded in FNITP. FNITP will develop the ability to link and access the scanned signed documents that reside in CIDM. This feature will allow FNITP to electronically monitor the occurrence of Section 32, 33, and 34.	Transfer Payment Director	October 31, 2007

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
Recommendation 9 - (Continued)	FNITP has the capability to enforce the use of formulas that derive what amount is being allocated to recipients. Unfortunately, these formulas differ from region to region due to provincial legislation which changes on a regular basis. In addition, not all program areas have clearly defined funding formulas related to their program. As program areas clearly define their funding formulas, FNITP will be configured to enforce the use of these formulas. An action plan will be developed which illustrates how the department will further define these formulas and enforce their use for recipient funding allocation.	Chief Financial Officer	March 31, 2008
	FNITP provides the capability for the department to monitor on-line if more than one arrangement was created for a recipient. In addition, FNITP warns the user if s/he encounters these situations. These changes represent significant improvements in the control over the creation of Funding Arrangements. These controls will be exercised to minimize the likelihood of creating more than one funding arrangement per recipient. The use of model agreements through FNITP has increased control as it allows the user to identify discrepancies between national models and regional operational needs. Controls ensure that the management control framework is being followed.	Transfer Payment Director	March 31, 2009

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System**
Region or Sector: **Chief Financial Officer Sector**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
Recommendation 9 - (Continued)	While the new level of controls implemented via FNITP have created operational challenges to both the Transfer Payments Directorate and the regions, they have permitted INAC to enforce greater consistency nationally.		
	Although the regions have some flexibility, the Transfer Payments Directorate now has a tool (FNITP) to monitor on-line models and arrangements. This will be the topic of future compliance activities by the Transfer Payments Directorate starting in Fiscal Year 2007-2008 subject to an annual risk assessment.	Transfer Payment Director	March 31, 2008
10. Manual controls should be developed and implemented for all Transfer Payments Directorate Management Control Framework control requirements that are not completely addressed by FNITP automated controls.	The observance of all Transfer Payments Directorate control requirements not embedded into the application will be reviewed in future compliance activities which will be carried out by the Compliance Unit of Transfer Payments Directorate starting in Fiscal-Year 2007-2008 subject to an annual risk assessment.	Transfer Payment Director	March 31, 2008
11. Considering the difficulties in trying to create FNITP user access profiles that match position titles, a segregation of duties conflict matrix should be developed to clearly document activities that need to be segregated. If conflicting responsibilities need to be given to specific users, monitoring controls should be implemented.	The lack of common organizational structure between regions and sectors makes this approach impractical. FNITP permissions were developed in such a way to accommodate the various organizational structures of regions. Permissions accesses are being monitored at the regional and national levels. Furthermore, FNITP has developed permission matrices reports to facilitate the monitoring of user access. Any further action is outside the scope of FNITP. This issue will be brought forward to the Senior Executive Committee prior to September 30, 2007.	Chief Financial Officer	September 30, 2007

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
12. Users should not be given the opportunity to modify FNITP variables that can create discrepancies between data in FNITP and the hard copy Funding Arrangements. In addition, as long as Funding Arrangements are in a status where they can be modified in FNITP, the printed Arrangements produced by the system should be clearly marked as draft.	The agreements are identified as draft until finalised. When finalised the agreements cannot be changed in the system. FNITP has provided a quantum leap improvement in the level of controls over the current business process. Although regions have some level of flexibility, for the first time Transfer Payments Directorate has a tool (FNITP) to monitor on-line the terms and conditions of funding arrangements Starting in Fiscal Year 2007-2008, this will be the topic of future compliance activities by the Transfer Payments Directorate subject to an annual risk assessment.	Transfer Payment Director	March 31, 2008
13. Exception reports should be developed and used to monitor control overrides. Furthermore, FNITP should force users to provide comments when overriding mandatory reporting requirements.	An exception report to monitor overrides will be developed in FNITP Version 2.0, which is scheduled for release in May 2007. The occurrence of overrides will be reviewed in future compliance activities which will be carried out by the Compliance Unit of Transfer Payments Directorate starting in Fiscal-Year 2007-2008 subject to an annual risk assessment.	Transfer Payment Director	March 31, 2008
14. The design of the FNITP application controls within the modules or functions that have not yet been developed should be assessed once the remaining functionality and controls are implemented, and before they are available for use.	A post implementation audit will be conducted at the end of the project (April 2008) to evaluate the status of the current observations and to verify new FNITP modules built in the upcoming Fiscal Year.	Director, Audit and Assurance Services	March 31, 2008

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
Project Management Controls 15. A "Go / No Go" decision framework should be developed and approved by the FNITP steering committee. The decision framework should be used to assess the project' s readiness for the planned go-live date.	A detailed "Go / No Go" checklist was developed in consultation with the Steering Committee. "Go / No Go" decisions will take place at four separate stages of the project as follow: • December 2006: Go Decision occurred Version1.0; • February 2007: Go Decision occurred Version1.25; • June 2007: Version 2.0; and • October 2007: Version 3.0.	FNITP Project Director	October 31, 2007
16. Knowledge transfer activities should be implemented within the Project Team to minimize dependencies on the project manager. Increased delegation should be a priority.	An approach to define the Support Model and Transition Approach was documented and presented to the steering committee on February 16, 2007. Workshops are planned for April and May 2007. The support model should be defined and approved by September 30, 2007.	FNITP Project Director	September 30, 2007
Data Input and Processing Controls 17. Until the reconciliation module is developed and implemented, reports from FNITP and the financial system should be compared on a regular basis to ensure that there are no discrepancies. The reports should be retained for audit trail purposes.	The reconciliation module will be functional by October 2007. In the meantime, users will be required to compare OASIS and FNITP financial reports to ensure that there are no discrepancies.	FNITP Project Director	October 31, 2007

Action Plan

Project Title: **System under Development Audit of First Nations and Inuit Transfer Payment System** **Project: 05/09**
Region or Sector: **Chief Financial Officer Sector**

Recommendations	Actions	Responsible Manager (Title)	Planned Implementation Date
Technical Vulnerability Controls 18. The department should formally sign-off on its acceptance of some of the risks identified in the FNITP Threat and Risk Assessment report, acknowledging its awareness of identified residual risks.	The threat and risk assessment action plan has been formally approved by the Chief Information Officer.	Chief Information Officer	January 31, 2007 (Implemented)