



Canadian
Heritage

Patrimoine
canadien

**REPORT ON THE
POST-IMPLEMENTATION AUDIT OF THE GRANTS AND
CONTRIBUTIONS INFORMATION MANAGEMENT SYSTEM
(GCIMS)**

CORPORATE REVIEW BRANCH

CANADIAN HERITAGE

February 25, 2004

Canada



TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
1.0 INTRODUCTION AND BACKGROUND	1
2.0 OBJECTIVES	1
3.0 SCOPE	2
4.0 METHODOLOGY	2
5.0 CONCLUSIONS	3
6.0 OBSERVATIONS AND RECOMMENDATIONS	4
6.1 Governance, Project and Risk Management	4
6.1.1 GCIMS Objectives and Goals	4
6.1.2 Accountabilities, Roles and Responsibilities	7
6.1.3 Project Planning and Information Technology Competencies ..	10
6.1.4 Project Planning and Risk Management	11
6.1.5 Tools and Reporting Mechanisms for Systems Performance ...	15
6.2 GCIMS Operations as an Effective Corporate Business System	16
6.2.1 Data Processing Environment	16
6.2.2 Consistent Application Version and Processing Platform	19
6.2.3 System Maintenance Strategy	21
6.3 GCIMS Effectiveness in Meeting Business Needs	22
6.3.1 Transfer Payment Policy	23
6.3.2 Meeting Business Needs	27
6.3.3 User Access and Security	32
6.3.4 Data Quality	34



EXECUTIVE SUMMARY

In accordance with the Department of Canadian Heritage's (PCH) Corporate Review Branch approved 2002-2003 Audit and Evaluation Plan, the Assurance Services Directorate undertook a post-implementation audit of the Grants and Contributions Information Management System (GCIMS). The requirement was established as a result of a department-wide program and corporate activity risk assessment.

The objective of the audit of GCIMS is to provide assurance on the adequacy of governance, project management and risk management practices, and to provide an overall assessment of the functionality of GCIMS as a corporate business system. The audit was conducted in the fall and winter, 2002-2003.

Based on the audit methodology employed, the audit team has determined that the governance, risk management and project management practices supporting GCIMS have a number of structural gaps that need to be addressed over the next twelve months as part of the GCIMS transition, and that while GCIMS is effective in processing grant and contribution data there are areas for improvement regarding compliance with the Transfer Payment Policy, data quality and security administration.

The governance, risk management and project management practices supporting GCIMS are not at the expected level of maturity. For example, a number of transition activities, including implementation of a GCIMS system maintenance strategy, will need to be addressed during the 15-month transition period. A formal GCIMS Steering Committee and GCIMS User Advisory Committee need to be formed. A GCIMS risk management regime and user roles and responsibilities need to be defined. Further, there is a need to introduce formal Service Level Agreements between GCIMS operators and users, and to revise the GCIMS Business Resumption Plan, especially with regard to new contact information, changes in technology and back-up support.

While GCIMS is an effective application in processing grant and contribution data, improvements are required regarding compliance with the Transfer Payment Policy, such as GCIMS users recording key performance related information into the application, the addition of a field in GCIMS to uniquely identify repayable contributions, and the incorporation of controls for more effective tracking and monitoring of advance payments.

Regarding data quality, a monitoring regime is required to ensure that payment information is reconciled between GCIMS and SAP, and the "clean-up" of grant and contribution data that preceded GCIMS needs to be addressed. Further, to strengthen security administration, formal procedures are required for the treatment of inactive

accounts in GCIMS, as are standards and procedures to guide managers /supervisors for assigning access rights and privileges to ensure appropriate access is given to GCIMS users.

The Audit Team has proposed 35 recommendations. These recommendations are intended to be used as a development guide for the GCIMS Transition Team over the course of the Transition Project. The recommendations are made with suggested time frames and relative levels of importance. Some high priority recommendations by suggested timeframe :

As Soon As Possible:

- Implement a GCIMS Risk Management Regime
- Assess the GCIMS Help Desk Workload
- Implement a GCIMS System Maintenance Strategy & Plan

Over the Next 5-12 Months:

- Complete Outstanding GCIMS Documentation
- Establish a GCIMS Steering Committee
- Establish a GCIMS User Advisory Committee

Long-Term:

- Implement Preventive System Controls in GCIMS for Advance Payments
- Implement a Direct Interface Between GCIMS and SAP



1.0 INTRODUCTION AND BACKGROUND

In accordance with the Department of Canadian Heritage's (PCH) Corporate Review Branch approved 2002-2003 Audit and Evaluation Plan, the Assurance Services Directorate undertook a post-implementation audit of the Grants and Contributions Information Management System (GCIMS). The requirement was established as a result of a department-wide program and corporate activity risk assessment.

GCIMS is a Department-wide, fully bilingual computer application built to facilitate the effective management and tracking of grants and contributions for all funding programs (approximately 50) administered by the Department of Canadian Heritage. It does so through a case-management process by capturing all steps involved in the project management process from the time a file is first opened by an officer to the time the file is officially closed.

GCIMS was developed in 1998-99 in the PCH Winnipeg Regional Office to replace the existing grants and contributions information management systems and was launched across the Department in September 1999. System management and development was transferred to Headquarters on January 1, 2003. The Finance Branch and the Knowledge and Information Technology Services (KITS) Branch are responsible for managing the system. Prior to GCIMS, there was no universal computer application in the Department that could allow comprehensive access to Grants and Contributions (G&C) data. GCIMS has introduced a reporting capability that allows users to generate a variety of reports pertaining to the Department's client base and to the projects for which these clients are funded.

The system currently manages approximately 12,000 payments totalling approximately \$530 million annually (1998/99 estimates) to provincial and municipal governments and to large and small arts, heritage, multicultural and sports organizations across the country. There are currently more than 976 active GCIMS accounts in the Department at headquarters and in regional offices.

Release 6.6, launched in August 2002, provided new functionality such as the incorporation of due diligence, data checking, validation and improved reporting. The current version of GCIMS (Release 6.7), launched in mid-December 2002, includes maintenance improvements primarily related to increasing the speed of the system.

2.0 OBJECTIVES

The objectives of the audit were to provide assurance on the adequacy of GCIMS governance, risk management and project management practices, and to provide an

overall assessment of the functionality of GCIMS as a corporate business system.

3.0 SCOPE

The audit examined the following:

- the management control framework surrounding the GCIMS governance structure and operations to-date, and whether it effectively manages and tracks departmentally-funded grant and contribution programs;
- the appropriateness of the management control and implementation frameworks around the effectiveness of ongoing application management, new releases and modifications; and
- its current use as an effective business operating system for the management of G&C programs.

The audit was conducted in the fall and winter, 2002-2003.

4.0 METHODOLOGY

The audit was conducted in accordance with the professional practice standards set out in the Treasury Board of Canada Secretariat's *Policy on Internal Audit* and by the Institute of Internal Auditors. The audit was conducted in three phases.

The *Planning Phase*, which included:

- a review of management, system, and related PCH and central agency documents;
- interviews with some 20 PCH management and staff, in headquarters and in the regions, with GCIMS responsibilities;
- obtained and assessed GCIMS documentation from the GCIMS Development Team in Winnipeg and from the GCIMS web-site;
- browsed the application using read-only rights; and
- examined a small sample of GCIMS data against source/hardcopy files.

The *Fieldwork Phase*, which included:

- new and follow-up interviews were conducted with responsible staff at headquarters and in the regions;
- project planning was assessed against the TBS Enhanced Management Framework for IT Projects;

- a checklist was developed to determine if GCIMS captures the critical elements and recommended practices of the Transfer Payment Policy;
- an end-user survey was conducted from various Program areas and Job groups across the country;
- previous audit reports were reviewed to determine if there was a change in user satisfaction on the issue of business needs;
- obtained the GCIMS database and the GCIMS data dictionary and ran queries using the audit software package Audit Command Language (ACL);
- reviewed “canned” and *ad hoc* reports generated from GCIMS and compared results to ACL queries;
- assessed GCIMS backup and the Business Resumption Plan for GCIMS; and
- reviewed test results with responsible staff on-site, in order to validate audit findings and conclusions.

The *Reporting Phase*, which included:

- development of a report summarizing audit conclusions and providing recommendations for improvement to system management practices.

5.0 CONCLUSIONS

The governance, risk management and project management practices supporting GCIMS were not at the optimal level of maturity. A number of transition activities, including implementation of a GCIMS system maintenance strategy, will need to be addressed during the 15-month transition period. A formal GCIMS Steering Committee and a GCIMS User Advisory Committee need to be formed. A GCIMS risk management regime and user roles and responsibilities need to be defined. Further, there is a need to introduce formal Service Level Agreements between GCIMS operators and users, and to revise the GCIMS Business Resumption Plan, especially with regard to new contact information, changes in technology and back-up support.

While GCIMS is an effective application in processing grant and contribution data, improvements are required regarding compliance with the Transfer Payment Policy, such as GCIMS users recording key performance related information into the application, the addition of a field in GCIMS to uniquely identify repayable contributions, and the incorporation of controls for more effective tracking and monitoring of advance payments.

Regarding data quality, a monitoring regime is required to ensure that payment information is reconciled between GCIMS and SAP, and the “clean-up” of grant and

contribution data that preceded GCIMS needs to be addressed. Further, to strengthen security administration, formal procedures are required for the treatment of inactive accounts in GCIMS, as are standards and procedures to guide managers /supervisors for assigning access rights and privileges to ensure appropriate access is given to GCIMS users.

The audit team has determined that the governance, risk management and project management practices supporting GCIMS have a number of structural gaps that need to be addressed over the next twelve months as part of the GCIMS transition, and that while GCIMS is effective in processing grant and contribution data there are areas for improvement regarding compliance with the Transfer Payment Policy, data quality and security administration.

6.0 OBSERVATIONS AND RECOMMENDATIONS

6.1 Governance, Project and Risk Management

Components of the management framework for GCIMS continue to be assembled and implemented as the GCIMS Transition Project works through its 15-month transition period schedule. A number of key components, including risk management, GCIMS user roles and responsibilities, and GCIMS objectives and goals, could enhance application governance if addressed in a more timely fashion than currently scheduled.

6.1.1 GCIMS Objectives and Goals

Criteria: Objectives and goals for GCIMS should be clearly defined, approved and effectively communicated.

GCIMS Goals and Objectives

The current objectives and goals of GCIMS have not been identified. KITS has developed a process to record application information for corporate systems, including objectives and goals, but no timetable has been identified to implement this process for GCIMS. Application objectives and goals are normally recorded in an application business case for system development. As GCIMS is not currently under development, the Transition Team is using the Project Approval Document (PAD) as the formal planning document for the transition. The PAD addresses the scope of the transition project but does not define objectives, goals and the future direction of GCIMS.



Without a formally approved vision for GCIMS, there is a risk of change in direction. If the objectives and goals of GCIMS are not articulated, corporate and user needs and expectations may not be met.

6.1.1.1 Recommendation

That the Director General, Financial Management Branch, in conjunction with Departmental senior management, identify, validate and formally approve GCIMS objectives and goals.

6.1.1.1 Management Response

Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and formulation of short, mid and long plans. Timeline: April 2004.

KITS drafted guidelines and a business case template for corporate application development in February 2003, however, this document has not yet been formally approved. A formal, evolutionary business strategy for GCIMS would provide the means to register the strategic direction of the system and to account for the ongoing business needs of the G&C Program areas and the Department.

6.1.1.2 Recommendation

That the Director General, Financial Management Branch develop and maintain a formal, evolutionary business strategy for GCIMS.

6.1.1.2 Management Response

Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and formulation of short, mid and long plans. Timeline: April 2004.



An approved IM/IT strategy, required to support strategic and long-term planning for corporate and other applications, has not been finalized and approved. Several IM/IT strategies were drafted in the past, however, these documents were not finalized and approved for implementation. The effort expended to produce these documents is not cost effective unless the documents are formally approved. Without approval, there is no assurance that the draft IM/IT strategy is aligned with departmental objectives or that it will be implemented. Long-term planning is essential to demonstrate results for effort and budgets expended, and to justify additional funding if needed.

6.1.1.3 Recommendation

That the Director General, Financial Management Branch confirm that GCIMS objectives are consistent with the approved IM/IT Strategy, when an approved IM/IT Strategy is available.

6.1.1.3 Management Response

PCH Senior Management must first confirm the need of an integrated IM/IT strategy, along with appropriate governance structures. Once in place, a related objective could be to ensure that GCIMS objectives are compatible.

GCIMS Communication Strategy

A GCIMS Communications Plan was drafted by the Financial Management Branch at the onset of the GCIMS transition in December 2002, identifying key information issues that need to be addressed and the strategy to target each audience. The Plan is not formally approved, however, nor is it detailed to identify deliverables, accountabilities and timelines. The purpose of an application communications strategy and plan is to guide internal communications activities throughout the deployment and ongoing upgrades of the application. A detailed and approved GCIMS Communications Strategy is required to provide assurance that the GCIMS Communications Plan complies with and communicates GCIMS goals and objectives and that deliverables are identified and implemented as planned. For example, under such a plan, newsletters on the Intranet would inform GCIMS users of the transition governance structure and the user support process. Without creation and formal approval of a communications plan, there is a risk that resources may not be allocated to implement the plan.



6.1.1.4 Recommendation

That the Director General, Financial Management Branch identify, validate and formally approve a GCIMS Communications Strategy and ensure the inclusion of and compliance with GCIMS objectives and goals.

6.1.1.4 Management Response

The Centre has recently established the position of Manager of Learning whose responsibilities will include formulation and implementation of a communications strategy tailored to the needs of GCIMS in particular and the G&C community within PCH in general and in line with PCH and FMB learning strategies. Timeline: April 2004.

6.1.2 Accountabilities, Roles and Responsibilities

Criteria: GCIMS accountabilities, roles and responsibilities should be clearly defined, rationalized and effectively monitored.

GCIMS accountabilities, roles and responsibilities are currently being developed and refined to address gaps resulting from the transition of GCIMS management from the Winnipeg Office to departmental headquarters. The GCIMS Project Charter, drafted in April 2002, has not been updated to reflect the new accountabilities and governance structure for GCIMS. A GCIMS Steering Committee and a GCIMS User Advisory Committee need to be formed to as part of the revised governance structure.

The GCIMS Transition Project was created in 2002 to develop the governance structure for the new GCIMS organization. A Functional Team and Technical Team were assigned from Finance and KITS, respectively, as co-leaders to manage the transition process. Formal approval of the GCIMS Transition Project was provided in the Project Approval Document (PAD), dated December 2002. The PAD broadly identifies the responsibilities of the ADM-Planning and Corporate Affairs, each Branch and the relevant committees. Corporate sponsorship, an essential governance requirement to provide management oversight and to ensure financial support, was provided via the PAD sign-off from the ADM-Planning and Corporate Affairs.

The Transition Teams are finalizing and addressing their detailed roles and



responsibilities for the management of GCIMS. Job descriptions formally define the roles and responsibilities for the Finance Transition Team and on a generic level for the KITS Transition Team. A technical team of indeterminate staff have been hired by KITS to support the production and operational needs of GCIMS.

Provision has been made in the PAD Resourcing Plan to retain the services of the Winnipeg staff for consultation. To ensure continuity of expertise and support, the Resourcing Plan identifies the need to retain the in-house project staff in either a line reporting or direct reporting relationship to KITS and to Finance. The Finance/KITS Team is staffed to provide Help Desk support to GCIMS users. KITS operations are organized on a matrix basis to facilitate resourcing and optimize skill sets for future GCIMS enhancements. As the GCIMS Team is currently being staffed, a comprehensive formal GCIMS Organization Chart does not exist. Once all detailed roles and responsibilities are finalized and approved, a GCIMS Organization Chart needs to be developed in order to communicate these accountabilities to the user community.

6.1.2.1 Recommendation

That the Director General, Financial Management Branch draft a comprehensive and formal GCIMS Organization Chart to identify all the key players involved in the transition (including the Committee Representatives), and a skills matrix to define the specific roles and responsibilities. The Organization Chart should be communicated on the GCIMS website as part of the Communications Strategy.

6.1.2.1 Management Response

Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and formulation of short, mid and long plans. Once the GCIMS Steering Committee is in place, PCH can then move on to confirming the organization structure required to meet business requirements. Timeline: April 2004.



The existing GCIMS Project Charter was developed when the system was managed by the Winnipeg Office. The Charter will need to be revised when accountabilities of the new GCIMS committee structure have been defined and all roles and responsibilities for GCIMS are formally approved.

6.1.2.2 Recommendation

That the Director General, Financial Management Branch and the Chief Information Officer, Knowledge and Information Technology Services revise the current GCIMS Project Charter to reflect the new roles and responsibilities of Finance, KITS, GCIMS Committees and the G&C Program areas, once these responsibilities are finalized and approved.

6.1.2.2 Management Response

KITS: KITS has the full compliment of staff as planned for under the GCIMS Transition 2003 Project fully engaged on GCIMS technical support and operations.

FMB: Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and formulation of short, mid and long plans. Once the GCIMS Steering Committee is in place, these elements, including an ongoing GCIMS Maintenance and Development Project Charter will be negotiated with KITS. Timeline: June 2004.

There is currently no GCIMS Steering Committee. A Steering Committee would serve to assess and approve GCIMS development priorities, act as a user interface to the departmental Investment Committee, and guide the GCIMS User Advisory Committee. The Steering Committee should be represented at the lower executive and middle management levels and be chaired, on a rotational basis, by a Program Director General from a GCIMS user area. The need for a Steering Committee has been identified by the Transition Team and the terms of reference are currently in the draft stage.



6.1.2.3 Recommendation

That the Director General, Financial Management Branch establish a formal GCIMS Steering Committee.

6.1.2.3 Management Response

Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and formulation of short, mid and long plans. Consultations are underway with program stakeholders to determine the most appropriate governance structure for the GCIMS. Timeline: April 2004.

The former GCIMS User Committee is inactive pending re-selection of membership and approval of new terms of reference. The need to revise the membership and responsibilities of the GCIMS User Committee was identified in the approved Project Approval Document, dated December 2002. The terms of reference of the GCIMS User Advisory were being drafted by the Transition Team. The accountabilities of the User Advisory Committee should identify ownership and key deliverables in order to ensure the G&C Program areas understand their responsibilities and appropriately select their representative for the Committee.

6.1.2.4 Recommendation

That the Director General, Financial Management Branch finalize the GCIMS User Advisory Committee roles and membership selection.

6.1.2.4 Management Response

Underway. The Centre of Expertise for G&C has already conducted high level consultations with program stakeholders to outline the vision for GCIMS, its ongoing goals, objectives and deliverables. The formation of the GCIMS Steering Committee will be tasked with confirmation of same and



formulation of short, mid and long plans. Consultations are underway with program stakeholders to determine the most appropriate governance structure for the GCIMS. Timeline: April 2004.

6.1.3 Project Planning and Information Technology Competencies

Criteria: The Transition Team members should have the required competencies in project management and information technology.

The GCIMS Transition Team members are trained in project management and information technology, and project management tools and standards are available at KITS. The Transition Team has the required expertise in project management and information technology to manage the GCIMS system. A Project Management Office (PMO) is established within KITS and the Project Manager for the PMO is a member of the GCIMS Transition Team. The Project Coordinator for the Transition Team is a Certified Project Manager (PMP) and the Finance Co-Leader is a former SAP Project Manager staff with the Department. Further, the Finance co-leader is an experienced manager with the required IT experience, with complementary skills in SAP and systems/financial controls.

6.1.4 Project Planning and Risk Management

Criteria: Project planning and risk management should be effectively applied.

Project management disciplines, in general, are rudimentary at this point in the GCIMS transition period but efforts are currently underway to implement recognized standards and best practices. A formal risk-management process is not in place.

Draft project management and systems development guides, methodologies and templates are available for managing corporate applications, however, the KITS Transition Team is currently managing GCIMS as a short-term operational activity using the “waterfall approach”. This approach identifies activities at an incremental level, rather than forecasting activities for the duration of the project. A high level work plan and Gantt Chart are provided with the PAD, however, detailed plans for the Transition Project have not been developed. Project management disciplines should be



systematically applied for the management of the GCIMS Transition Project to ensure the Project is efficiently resourced and costed and that activities are managed in a proactive manner.

6.1.4.1 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services apply recognized project management standards and tools to the planning of the Transition Project in order to provide a detailed work plan for the duration of the GCIMS Transition Period.

6.1.4.1 Management Response

KITS: The GCIMS Transition 2003 Project as approved by the ADM of the Planning and Corporate Affairs Sector on Dec. 20, 2002 was successfully closed ahead of schedule as of the end of F/Y 2002/2003. A final report was issued to management at that time. As of April 1, 2003, the support for GCIMS has continued under the auspices of general operational management practices.

A formal risk management strategy and process are not in use. The GCIMS Transition Project Manager acknowledged the need for a formal risk assessment for GCIMS, however, a timeslot has not been identified. Risk management is essential to identify the vulnerabilities of the application and the management controls required to ensure sound decision-making and planning. The risk management process requires identifying a schedule for action. A GCIMS Risk Assessment study was conducted in 2001. Several of the system-related observations raised are still outstanding. Examples include the absence of a specific strategy, a detailed Project Plan, a Service Level Action Plan, resolution of integrity issues concerning historical data, and the lack of a Business Practices Manual. Also noted was the risk of maintaining more than one system for data entry of grants and contribution transactions, including SAP, the manual GCIMS system, and the Programs own satellite system(s).

6.1.4.2 Recommendation

That the Director General, Financial Management Branch implement a business risk management strategy and ongoing



risk management process for GCIMS. The risk management strategy should identify the points at which a comprehensive risk management assessment is to be applied.

6.1.4.2 Management Response

Agreed. The formation of the GCIMS Steering Committee will be tasked with development and implementation of a business risk management strategy and ongoing risk management process for GCIMS which should identify the points at which a comprehensive risk management assessment is to be applied. Timeline: September 2004.

6.1.4.3 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services, implement a technical risk management strategy and ongoing risk management process for GCIMS. The risk management strategy should identify the points at which a comprehensive risk management assessment is to be applied.

6.1.4.3 Management Response

This to be coordinated with FMB and CEG&C as per 6.1.4.2 above. Timeline: S

KITS acknowledges the requirement for a risk assessment including a Threat and Risk Assessment, TRA, against the vulnerabilities of the application. KITS assesses such as part of the Government of Canada's IT Security Policies, every two years, which completes a security audit of the departmental technical infrastructure.. The application is not exposed to the public via extranet or VAN or any other means, so external security vulnerabilities are not a threat under these conditions. Such technical metrics as application availability relate to maintainability, serviceability and reliability and as of transition, KITS has increased the availability of GCIMS by addressing these issues.



A new technical environment will be in production as of Oct 18, 2003, which will physically separate the test and training environment from the production environment. The previous production environment was four years of age and did not have the latest Microsoft database version, O/S or updated security releases. As well, the previous production environment incorporated the test and training environment on one physical server and on more than one occasion this caused downtime to the production environment. Also to minimize risk KITS has severed the outside vendor, On Line Business Systems from network access to the production environment. As well, the new technical environment increases the availability of GCIMS by implementing full hardware, O/S and specific application monitoring services that notify KITS technical support in the event of a GCIMS service outage.

End user security rights and privilege access is a responsibility of FMB

Two key management risks identified during the audit were the lack of applied corporate documentation standards and a formal review process to ensure an adequate management trail of activity. Documentation standards were not consistently applied (i.e., the date of document preparation, ownership, status, version, sign-off, and distribution). Minutes were not systematically recorded and, when recorded, did not consistently identify timelines, accountabilities or concrete deliverables. Several GCIMS deliverables were produced but were not formally approved or implemented.

Two key management risks identified during the audit were the lack of applied corporate documentation standards and a formal review process to ensure an adequate management trail of activity. Documentation standards were not consistently applied (i.e., the date of document preparation, ownership, status, version, sign-off, and distribution). Minutes were not systematically recorded and, when recorded, did not consistently identify timelines, accountabilities or concrete deliverables. Several GCIMS deliverables were produced but were not formally approved or implemented.



6.1.4.4 Recommendation

That the Director General, Financial Management Branch and Chief Information Officer, Knowledge, Information and Technology Services institutionalize documentation standards for uniformity and completeness of corporate deliverables, and formalize the review and decision-making processes.

6.1.4.4 Management Response

KITS: KITS has implemented a formal change management process against GCIMS and an approved document must be completed if any changes are made to the technical production environment. Only KITS has full rights to this environment. This was not the case prior to transition.

FMB: Both the GCIMS Unit of the Centre of Expertise for Grants and Contributions and the system development unit of KITS responsible for maintenance of the GCIMS have reviewed documentation standards for GCIMS and have introduced a change management process which documents requests for modifications to the GCIMS platform as well as an approval process and sign-off authorization for work done.

Concerted effort is being expended by KITS to develop a corporate system development methodology as well as several key GCIMS documents, including the GCIMS User and Sub-System Manuals, the GCIMS Data Dictionary, and the GCIMS Documentation Strategy that identifies the key documents required for Developer, System and User activity. The GCIMS Documentation Strategy was found to be very comprehensive and consistent with industry standards. The Documentation Strategy should be applied as a corporate documentation standard for all corporate applications.

6.1.4.5 Recommendation

That Chief Information Officer, Knowledge, Information and Technology Services ensure that GCIMS deliverables identified in the GCIMS Documentation Strategy is completed, formally approved and implemented.

6.1.4.5 Management Response



KITS: At KITS, documentation standards and procedures are being drafted as part of the effort to complete a branch wide hardware, software or service release to production methodology. Such documentation as User Guides and Technical Standards and Procedures are being developed.

FMB: Both the GCIMS Unit of the Centre of Expertise for Grants and Contributions and the system development unit of KITS responsible for maintenance of the GCIMS have reviewed documentation standards for GCIMS and have introduced a change management process which documents requests for modifications to the GCIMS platform as well as an approval process and sign-off authorization for work done.

6.1.5 Tools and Reporting Mechanisms for Systems Performance

Criteria: Tools and reporting mechanisms should be in place to measure and report on the performance of the system.

No departmental user-related performance indicators or quality criteria are applied to help manage the GCIMS system. The performance of GCIMS is currently monitored based on the performance of the data processing environment (i.e., network, servers and hardware). User-related performance metrics for GCIMS (e.g., no. of users on the system, no. of active accounts, no. of failed access attempts, no. of system access changes requested and granted, and printing problems) are not actively identified and monitored. Without such performance metrics, there is no detection control to signal functional problems in a timely manner and to assess if service levels and quality criteria are met. As a result, user support remains reactive in nature, extra effort is unduly applied to the Help Desk, long-term planning is compromised, and corporate IT service delivery is questioned.

6.1.5.1 Recommendation

That the Director General, Financial Management Branch, in conjunction with the Chief Information Officer, Knowledge, Information and Technology Services, introduce user-related performance metrics as a work discipline and a corporate reporting requirement for GCIMS. Performance metrics for



GCIMS could be integrated into performance contracts.

6.1.5.1 Management Response

KITS responded to the FMB request to remove inactive user accounts by implementing an automated service that runs once per day to remove accounts that have not been logged into for 400 days. If requested by FMB, KITS would be pleased to look at automating other user related performance criteria.

FMB: Service delivery standards will be developed and proposed to the GCIMS Steering committee for confirmation. System availability standards and system response time benchmarks for the various locals for PCH will also be established and monitored, with regular reporting to the GCIMS Steering committee as required. Timeline: September 2004.

6.2 GCIMS Operations as an Effective Corporate Business System

GCIMS is not yet operating as an effective corporate business system. A number of transition activities, including establishment of a formal and consistent data processing environment, a consistent application version and platform, and a system maintenance strategy, will need to be implemented during the GCIMS transition period.

6.2.1 Data Processing Environment

Criteria: The application should operate in a formal, fully supported and monitored data processing environment.

The data processing environment at KITS has not been formalized for GCIMS. Specifically, a Service Level Agreement (SLA) was not in place between KITS and GCIMS users. As a result, the Transition Team was developing processes for the Help Desk to develop management controls for GCIMS and to identify and formalize Help Desk support for the GCIMS user community. The Finance Team is over-tasked with the Help Desk function and there is a risk that the level of support provided to the user community may deteriorate. The KITS Business Resumption Plan dated April 2002 needs to be updated to reflect new responsibilities and support contacts at

headquarters.

A Service Level Agreement is required to communicate the roles and responsibilities of each support group (e.g., application support, help desk and operations support), the level of service to be provided (e.g., hours of service, response time, scope of service), the problem management process and escalation procedures, and the performance metrics to be collected to ensure the service provided complies with the agreement.

There is no SLA in place between KITS and GCIMS users. An Operational Level Agreement was drafted in October 2002 for all corporate applications in KITS, however this agreement has not been formally approved and implemented. The GCIMS Transition Team identified, in their Minutes, the need to develop a Service Level Agreement for GCIMS to determine the quality and service levels required. A timetable was not identified for this activity. Without an approved Service Level Agreement, there is no assurance that the support provided for the GCIMS system will be responsive to the users needs and that problems will be channeled to the appropriate support group and resolved in a timely and cost effective manner.

6.2.1.1 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services develop, validate and formally approve a GCIMS Service Level Agreement(s) between KITS and GCIMS users.

6.2.1.1 Management Response

KITS is not directly responsible for service level agreements to the end user. KITS works with FMB in this regard, through services provided by the KITS PCH Help Desk. Such services are defined around specific response times and escalation procedures. KITS does provide a BRP and this document is being updated on or before the end of November 2003.

FMB: The functional authority for day to day management of the GCIMS rests with the Manager, GCIMS. Efforts have be initiated with KITS to determine the best instrument (Service Level Agreement, Memorandum of Understanding, Project Management Charter, etc.) to budget, plan and control expenditures related to the ongoing maintenance and



refinement of the GCIMS application within PCH. Also need to determine whether these instruments constitute bi-lateral (FMB & KITS) or tri-partite (FMB, KITS, GCIMS Steering Committee) agreements. Options will be presented to the GCIMS Steering committee for decision. Timeline: September 2004.

GCIMS is co-managed by the KITS Help Desk for technical and systems issues, and the Finance Help Desk for user access and functionality issues. One resource was provided for the Finance Help Desk (i.e., since the start of transition). The workload for the Help Desk has been compounded by the heavy volume of access profile changes and the task of data backfill from the SAP application. As a result, the Finance Team is over-tasked with the Help Desk function and there is a risk that the level of support provided to the user community may deteriorate. The resourcing levels of the Finance Help-Desk may not be adequate to provide continuous and responsive service support to the user community.

6.2.1.2 Recommendation

That Director General, Financial Management Branch develop a detailed work plan for the workload requirements of the Help Desk in order to estimate and cost the resources required to staff the function.

6.2.1.2 Management Response

Measures are underway to normalize the organization and resources of the GCIMS Unit, including the GCIMS User Help Desk. Formal working relationship and assignment of areas of responsibility within the context of users support have been negotiated and implemented with regards to the GCIMS User Helpdesk, the KITS Helpdesk, GCIMS Functional DBA and the KITS Development Team and will be formalized through a memorandum of agreement in the near future. Timeline: September 2004.

The Business Resumption Plan (BRP) for KITS is not up-to-date. The BRP was last revised in April 2002 when GCIMS was managed by the Winnipeg Office. The Plan included a responsibility matrix and contact information. The Plan did not reflect the



new organization or staff and should to be revised once the detailed GCIMS governance framework is finalized and approved.

6.2.1.3 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services revise, validate and formally approve the GCIMS Business Resumption Plan, especially with regard to contact information and relevant changes in technology, application versioning and back-up support.

6.2.1.3 Management Response

KITS has a formal Business Resumption Plan which is revised annually and which will be updated on or about the end of November 2003 to reflect changes to the GCIMS technical environment as well as technical contacts.

FMB: A Business Resumption Plan will be developed in consultation with KITS to ensure that the specific requirements of the GCIMS are addressed and a recommendation will be presented to the GCIMS Steering committee for decision. Timeline: March 2005.

6.2.2 Consistent Application Version and Processing Platform

Criteria: One version of the application should be implemented on a consistent desktop platform, network infrastructure and telecommunications environment.

GCIMS is not running on a consistent desktop platform across the country. In addition, a report of access profiles dated December 2002 indicated that the version of GCIMS in use is not consistent. Both issues, where the version or desktop are below departmental standard, caused corporate support groups and affected users with some minor delays in problem identification and problem solving. In the short-term these problems are accepted by the user community as a nuisance that can be dealt with, however, in the long-term there can be a significant impact on productivity (e.g., would limit system integration).

Desktop platform standards are required to ensure interoperability and effective



information exchange across the department and to provide for the cost-effective use of desktop support. Desktop standards are documented on the KITS website, however, there is no policy or implementation plan to ensure compliance with these standards. There is a risk that the lack of enforced departmental standards may influence the continued use of non-standard desktop configurations which in turn will require additional resources and skill sets to support.

6.2.2.1 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services develop a policy to mandate the standardization of the desktop platform and to direct that non-standard platforms will not be supported by the KITS Help Desk by a specified cut-off date.

6.2.2.1 Management Response

KITS have formulated a policy to address this issue and are currently in the process of updating all workstations to a consistent standard.

A snapshot review of the access records for the 650 GCIMS users during December 2002 revealed that various versions of GCIMS were assigned or in use for several users. To optimize the utility of systems enhancements and to ensure uniformity of data content and format, the latest version of GCIMS should be implemented for all users.

6.2.2.2 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services investigate the discrepancy of application versions reported on access profiles and prepare an action plan to redress the problem of GCIMS versioning.

6.2.2.2 Management Response

KITS manages the version of the GCIMS client, which is pushed to the desktop upon log on to GCIMS. Upon logon the application automatically checks and detects whether the current client installed on the desktop is the most recent version and automatically installs if not. It is not technically



possible to run a client other than the most recent version, unless the desktop is not connected to the network, in which case, the usability of the application is minimized. An end user is assigned a security profile with specific rights to read or write to specific areas or records within GCIMS. This is a standard approach to access within a business system.

FMB: A key feature of GCIMS is that all users logging into GCIMS use the most current version of GCIMS. In preparation for the recent release of the GCIMS upgrade on October 17, 2003, the status of all users was confirmed and any discontinued accounts were disabled.

6.2.3 System Maintenance Strategy

Criteria: The application should be in operation under a formal, verified and approved maintenance strategy.

A current, formally approved maintenance strategy was not in place for GCIMS. A formal maintenance strategy should be in place in order to efficiently and effectively identify, plan and deliver emergency fixes, enhancements, new versions and supporting documentation, as well as the inventory of related assets and technological changes required to provide continued processing and support for an application. A formal maintenance methodology should also address change request approval documents and processes, configuration management, test strategies and documentation standards. Without such a strategy, required changes may not be identified, prioritized, resourced or implemented in time to meet business needs.

6.2.3.1 Recommendation

That the Director General, Financial Management Branch and the Chief Information Officer, Knowledge, Information and Technology Services develop and implement a system maintenance strategy to deliver the outstanding enhancement requests for GCIMS. The strategy should also provide for the inventory and control of the various operating systems in use and a resourcing strategy to retain corporate memory.

6.2.3.1 Management Response



KITS has implemented a formal change management process against GCIMS and an approved document must be completed if any changes are made to the technical production environment.

Several initiatives were underway in KITS, however, to develop a formal maintenance strategy and methodology. A Change Control Board has been created to manage enhancements of corporate applications. Planning is underway to implement an industry-recognized best practice for configuration management (i.e., the Information Technology Infrastructure Library (ITIL) methodology). A draft release and change management strategy and several supporting templates, such as the formal change request, project initiation approval and project status report documents, are underway or in use for the maintenance of other corporate applications.

See 6.1.1.1 and 6.2.1.1 above. The Centre of Expertise for Grants and Contribution has embarked on a comprehensive review of the current practices and requirements with respect to the management of Grants and Contributions with the aim of a return to reasonable diligence. Once completed, all finding and recommendations will be presented to a GCIMS Steering Committee, struck by senior management to develop and confirm the strategic direction for G&C Management, the use of tools such as the GCIMS and integration of initiatives with the overall IM/IT Strategy of the department. In addition, the steering committee will establish the process for the management of all recommendations for change or enhancement to the GCIMS. Timeline: September 2004.

Several initiatives were underway in KITS, however, to develop a formal maintenance strategy and methodology. A Change Control Board has been created to manage enhancements of corporate applications. Planning is underway to implement an industry-recognized best practice for configuration management (i.e., the Information Technology Infrastructure Library (ITIL) methodology). A draft release and change management strategy and several supporting templates, such as the formal change

request, project initiation approval and project status report documents, are underway or in use for the maintenance of other corporate applications.

6.3 GCIMS Effectiveness in Meeting Business Needs

GCIMS is an effective application for processing grant and contribution data, however, areas for improvement exist with regard to the Treasury Board (TB) *Policy on Transfer Payments* (PTP), meeting corporate business needs, security administration and data quality.

6.3.1 Transfer Payment Policy

Criteria: GCIMS functionality should be compliant with the Treasury Board *Policy on Transfer Payments*.

GCIMS incorporates most of the key elements outlined in the PTP, however, information such as advance payments, repayable type contributions and results-based monitoring at the corporate level are not available.

Results Measurement

A key element of the PTP is the existence of an appropriate performance framework for measuring results. Performance measurement is vital in determining if the expected outcomes and activities have been achieved towards the success of the Program. A Performance Measurement Framework (PMF) function was built into GCIMS that captures the activities and expected outcomes of a project.

6.3.1.1 Recommendation

That the Director General, Financial Management Branch, direct GCIMS users to complete performance management information in the PMF function.

6.3.1.1 Management Response

Upon formation of the GCIMS Steering committee and in conjunction with the review of grants and contribution processing currently underway, the subject of inclusion of performance measurement data within the GCIMS application



**or some alternative instrument will be assessed. Timeline:
September 2004.**

The information recorded in PMF is captured at the project level in a manner that cannot currently be rolled-up for reporting purposes (i.e., information is recorded mainly in a textual format). As a result, it is difficult to measure expected outcomes, and the overall success and effectiveness of Programs. Results-based management and accountability framework information for measuring and reporting of results, a critical component of the PTP, is therefore not available to senior management for reporting at the corporate level.

6.3.1.2 Recommendation

That the Director General, Financial Management Branch, investigate a means to roll-up textual information in GCIMS so that senior management can gage the effectiveness of the Programs. For example, a table could be added to GCIMS that translates the activity and expected outcomes into numeric information.

6.3.1.2 Management Response

See also 6.3.1.1 above. Once the Executive Committee for the department has finalized and confirmed the PRAS and KPRS structures for PCH, where applicable, options for addressing these requirements within GCIMS will be presented to the GCIMS Steering committee for decision. Timeline: September 2004.

Advance Payments

GCIMS currently does not have any way to track advance payment information. Prudent cash management policy discussed in the PTP states that payments should not be paid to recipients in advance of need and should be timed to correspond as closely as practicable to a recipients flow requirements. GCIMS does not have a preventative control to warn users that advance payments have exceeded the financial thresholds described in Schedule B of the PTP. SAP is also unable to identify advance payments. Advance payments present a significant element of risk to the Department in the event that a project is abruptly terminated as a result of non-compliance to the terms and



conditions of the contribution agreement. For example, risk of non-recovery is greater where excessive prepayments are made (in excess of threshold amounts established in Schedule B of the PTP) and the recipient is not able to reimburse. The only compensating or detective control at this time is through the monitoring or post-audit exercise undertaken by the Finance Branch.

6.3.1.3 Recommendation

That the Director General, Financial Management Branch, in consultation with the Chief Information Officer, Knowledge, Information and Technology Services, incorporate preventive controls into GCIMS for advance payment information in order to allow advance payments to be more effectively tracked and monitored.

6.3.1.3 Management Response

KITS, once requested through FMB, would assess the impact to GCIMS to respond to these business requirements and determine the possibility of incorporating these features into the application.

Agreed. The actual solution will require additional analysis of options and instruments available. Coincides with implementation of SAP 4.7. Timeline: March 2005

Repayable Contributions

GCIMS nor SAP identify repayable contributions. Departments are charged with establishing policies and procedures to ensure that where a contribution is made to a business and intended to allow the business to generate profits or to increase the value of the business, the business is required to repay the contribution. It is difficult to track repayable type contributions in order to determine the effectiveness of this type of contribution and, also, when the repayments should be made.

6.3.1.4 Recommendation

That the Director General, Financial Management Branch, add a field in GCIMS to uniquely identify repayable contributions.



6.3.1.4 Management Response

Agreed. The actual solution will require additional analysis of applicability to PCH programs, identification of required controls and associated business rules and assessment of impact on existing operations. Timeline coincides with implementation of SAP 4.7. March 2005.

Conflict of Interest

GCIMS does not have a system-generated disclaimer for the Conflict of Interest and Post-Employment Code for Public Office Holders and the Conflict of Interest and Post-Employment Code for the Public Service. A disclaimer, related to the conflict of interest guidelines, would serve to remind employees of their ethical responsibilities as public administrators. While no specific issues were identified as a result of not having a disclaimer, PTP suggests a disclaimer be presented to users as part of the grants and contributions process.

6.3.1.5 Recommendation

That the Director General, Financial Management Branch, consider adding a Conflict of Interest disclaimer to GCIMS, to remind employees of their role and responsibilities when administering grants and contributions.

6.3.1.5 Management Response

This recommendation will be presented to the GCIMS Steering Committee for their consideration. Timeline: March 2004.

Monitoring and Audit

There is no audit module, or similar functionality, in GCIMS to record the results of ongoing monitoring and audit activity. Departmental internal audit plans must include a provision for the review of internal management policies, practices and controls of transfer payment programs. Management would significantly benefit from the addition of a GCIMS Audit Module/Tab that records the results of, and effectively monitors, Program strategy and department audits. With an Audit Module in GCIMS, the Department could gauge the efficiency and effectiveness of the G&C delivery process.

The extent of active monitoring and the level of examination of contribution recipients cannot be determined effectively with GCIMS as currently designed.

6.3.1.6 Recommendation

That the Director General, Financial Management Branch, incorporate an Audit Module into GCIMS to effectively record the results of monitoring/audit of contribution agreements.

6.3.1.6 Management Response

Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: September 2004.

6.3.2 Meeting Business Needs

Criteria: The design/functionality of GCIMS should meet user needs.

Overall, the design and functionality of GCIMS meets user needs. This conclusion is consistent with previous reports/audits of GCIMS. Areas for improvement exist, however, with respect to reporting, timeliness of payment information, French language in GCIMS, and navigation. The assessment of GCIMS functionality/design was divided into six areas of the application, as follows:

- Navigation
- Data Entry
- Case Management
- Reporting
- Security
- System Administration & System Maintenance

Navigation

Navigation (moving from screen to screen) through GCIMS operates through as a series of functional modules, which makes the application easy to use/navigate. Navigation in GCIMS was found to be slow, however, especially with other applications running on the workstation. In addition, GCIMS has a tendency to “freeze” or lock-up



when operating on Windows 95 or 98, but not with Windows 2000. (See 6.2.2.1 in Section 6.2.2, above).

One GCIMS project can be open at a time, requiring the user to completely close the current project in order to open a new project. In addition, with GCIMS tabs, the user must scroll down one window before they can get to the next window (i.e., there is no ability to go directly to the desired screen). Further, some GCIMS tabs have multiple windows within one view, which forces the user to scroll down in order to view the information. A lot of time is spent navigating in GCIMS, particularly with respect to opening and closing projects, as there can be more than one project associated with a given client.

6.3.2.1 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services implement functionality, with appropriate controls, to allow users to view and update multiple projects related to a given client.

6.3.2.1 Management Response

KITS is currently investigating the possibility of adding enhancements to GCIMS to accommodate a number of user views and amalgamation of information. The application was designed with a single project and a single application basis and with this approach there may be architectural reasons why such a request may or not be accommodated. Regardless, via reporting, this information is obtainable.

FMB: Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: September 2004.

Data Entry

Data entry is well controlled in GCIMS, as data is processed through a single point of entry (i.e., only the officer of record can enter data). Users are permitted to add, edit or delete the data they have created. Other users' signoffs can be viewed.

A lot of data is required to process a project from start to finish, requiring a lot of data entry. Users have noted the considerable time/level of effort required enter data into GCIMS. As a result, the extent and consistency of data being entered into “open” or text fields varies by user

Case Management

GCIMS has excellent case management functionality, including:

- *Workflow*: Workflow interfaces efficiently so that users can move a grant or contribution project file through the various workflow processes required during the life cycle of a project. Workflow is divided into a series of tabs which help define the work to be done on each tab.
- *Due Diligence*: Workflow forces users through a series of business activities a project file must follow in order to be approved.
- *File Routing*: File Routing allows ownership of a file to be transferred to other users of the system. The electronic routing of files is tracked in the system and allows authorized users to complete their work on the file.
- *File History*: File History provides the complete history of a file, including who has updated or edited project information and, therefore, provides a good management trail.

Reporting

GCIMS captures a wide range of information on recipients and provides significant opportunities for data mining. Users are selecting the data elements they need for reporting and for supporting business decisions. There are two types of reports available in GCIMS: existing or “canned” reports that offer the user a wide variety of information on client an/or individual projects and applications; and *Ad hoc* reports that give the user the flexibility to choose their own criteria based on business need.

GCIMS, however, is not meeting the full range of corporate reporting needs. GCIMS has the potential for data mining and therefore, could offer the user the flexibility to select and choose data elements to meet business needs. Currently, data must be extracted from the GCIMS database and independently manipulated by users. User success with this type of reporting is dependent upon the complexity of the information sought and the skills of the individual performing the exercise. Specifically:

- Report generation and printing can become very slow if there is a lot of activity on GCIMS.
- The slow processing speed when using GCIMS remotely is a significant



disincentive for using the application remotely, therefore in some instances, GCIMS teleworking could be an unproductive effort.

- Existing GCIMS reports frequently do not address user and corporate needs. Special reporting requests are frequently required and are often time consuming to complete as significant time is required to manipulate GCIMS data in order to prepare it for reporting.

6.3.2.2 Recommendation

That the Director General, Financial Management Branch consider the development of system functionality that would allow users to select data fields from a pick list. This would give users more flexibility to customize their reports and address business needs.

6.3.2.2 Management Response

Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: March 2004.

- Users noted a lack of confidence in the completeness and accuracy of financial data in GCIMS. As a result, users refer to SAP for GCIMS financial information. Users are required to enter the same payment information into both GCIMS and SAP. The risk of double entry of financial information is that the secondary system (GCIMS) is not updated concurrently with the primary system (SAP) resulting in timing issues around payment information. Consequently, no reliance is placed on the financial information in the secondary system; and
- Extra time and effort is required to support payment information in GCIMS. The duplication of payment information into both SAP and GCIMS will continue, however, until an automated interface is implemented between the two applications to exchange financial transactions.

6.3.2.3 Recommendation

That the Director General, Financial Management Branch, directly interface GCIMS with SAP for the exchange of financial transactions. This interface would improve the timeliness and reliability of payment information in GCIMS and eliminate the current duplication of effort for data entry.



6.3.2.3 Management Response

See also 6.1.2.1 and 6.2.3.1 above. This requirement to expand the existing interface between SAP and GCIMS, along with assessing the potential impact of the SAP upgrade to version 4.7 has been identified as a priority and analysis of requirements and evaluation of options is underway. Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: March 2005.

Security

Overall, GCIMS has well designed security controls, however, management around these security controls needs to be strengthened. Application security is used to control access to different parts of the application, including limiting access to project and applicant data. Security components include blocked read and write access to projects, tracking of individuals that have had write access to a projet, tracking of individuals who have key decisions, and creating historical logs of each project as it progresses to completion.

Access to GCIMS data is restricted through the use of database passwords and network security. Further, protected information associated with a registered user is not accessible by unauthorized staff unless granted by the user.

In order to transfer application ownership of a GCIMS file from one user to another, special permission is required in the system. GCIMS files cannot be transferred to users who do not have the security rights to work on the file. Unauthorized users are automatically filtered out from the list of possible transferees.

Application security is managed through several administrator levels having access to different configuration options. Changes to the application are tracked and recorded in the application log. Log reports that identify failed access attempts are not currently being monitored. As a result, common security risks such inappropriate activity by staff or contractors is not identified.

System Administration & Systems Maintenance

The application files and production data are backed-up on-site on a daily basis. Data media, including tapes used to backup data tables and application log files, that include archived logs containing Protected level "B" information, are stored as required in a



secure facility. GCIMS production data and source code are backed-up daily. A copy of both the production data and source code are maintained off-site.

GCIMS can generate a number of relevant application-related event logs, that are useful in identifying potential operational, security and management issues. Log files are separated into two groups: System Events and Business Events. The System Event log captures events related to specific functions (e.g., running an operating system or an application error occurring). The Business Event log records events such as the registration of a new user, log-in date and time, failed login attempts, password reset events and or similar activities. The System Event log, generated by GCIMS and maintained in the operating system, helps the support team detect and debug application errors. The Business Event log provides a chronological history of business transactions, including ad-hoc queries.

GCIMS functions in both English and French. Users noted dissatisfaction with the French language version of GCIMS, for example, how business rules in English have been improperly translated into French and errors with the bilingual spell checking feature. Poor translation has not impacted the administration of grants and contributions.

6.3.2.4 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services review French language text and the spell checker in GCIMS to ensure that linguistic rules have been respected.

6.3.2.4 Management Response

The GCIMS Unit within the Centre of Expertise has initiated a review of all English and French language text employed within the GCIMS application. The feasibility of incorporating enhanced spell-checker technology within the GCIMS application will be assessed by KITS and available options and associated costs will be presented to the GCIMS Steering committee for decision and determination of relative priority. Timeline: March 2004.

6.3.3 User Access and Security

Criteria: Administration of user accounts in GCIMS should be effectively managed.

Administration of user access in GCIMS is not effectively managed. A number of changes are required, including formal documentation of GCIMS access requirements by position, mandatory completion of the Job Description field, and strict management of inactive accounts.

Access to GCIMS is currently managed centrally by Finance. Users apply for access to GCIMS through the PCH intranet site. Access rights and privileges are assigned based on the user's Program area and position. Access rights and privileges are verified with the user's supervisor/manager on a limited basis, to ensure that the user has the appropriate access to do their job. There is insufficient documentation, however, to guide managers and supervisors to ensure that access rights and privileges have been appropriately assigned for a given position (e.g., program officer, administrative or finance clerk, analyst, communications officer or finance officer) and to ensure appropriate segregation of duties. Without standards or guidelines to manage access rights and privileges, it is difficult for managers and supervisors to determine if the appropriate permissions have been assigned.

6.3.3.1 Recommendation

That the Director General, Financial Management Branch, establish standards that guide managers/supervisors for assigning access rights and privileges to ensure that appropriate access is given to users.

6.3.3.1 Management Response

The GCIMS Unit within the Centre of Expertise has initiated a review of current user access rights and privileges with the aim of establishing a reference guide based on job functions (e.g.: Director General, Director, Program Manager, Team Leader, Program Officer, Program Support, Financial Administration, System Administration, Secretariat, etc.). A number of improvements to the management and administration of user accounts have recently be implemented. Timeline: September 2004.

GCIMS has a Job Description field that is not regularly completed. The Job Description field, which is not mandatory to complete, can be used in comparison with the user's



access privileges to determine the correctness of assigned privileges. Without this field being populated on a consistent basis it is difficult to monitor/determine if the appropriate access rights have been assigned. The potential impact of inappropriate access privileges includes inappropriate viewing of confidential client information, the ability to make unauthorized changes to accounts, and the ability to delete files without permission.

6.3.3.2 Recommendation

That the Director General, Financial Management Branch make the Job Description field in GCIMS a mandatory field.

6.3.3.2 Management Response

Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: September 2004.

There was no process for formally addressing inactive user accounts. There were no reports used by management to monitor inactive user accounts. Several GCIMS users were categorized as active in the system but had not logged into GCIMS for more than one year. There was no formal procedure in place to disable user accounts when an employee leaves the Department. Disabling of GCIMS account is not included in the HR Exit Checklist. The potential for unauthorized access is present if inactive accounts are not regularly monitored and disabled.

6.3.3.3 Recommendation

That the Director General, Financial Management Branch, formally document procedures (that would include monitoring) to address inactive accounts - reports identifying inactive accounts should be reviewed by each G&C Program area to ensure all inactive accounts are addressed.

6.3.3.3 Management Response

Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: September 2004.



The Business Resumption Plan (BRP), that includes the GCIMS application, has not been tested in the recent past. Without periodic testing of application recovery, there can be no assurance that the Business Resumption Plan will functioned as designed.

6.3.3.4 Recommendation

That the Chief Information Officer, Knowledge, Information and Technology Services identify the test schedule for the GCIMS BRP and document test results.

6.3.3.4 Management Response

KITS has a BRP procedure of which a revision is pending and to be completed on or about the end of November 2003. The testing of such a plan against the IM/IT infrastructure inclusive of GCIMS has not yet been scheduled, however, specific procedures are tested during scheduled maintenance shutdowns.

FMB: A Business Resumption Plan will be developed in consultation with KITS to ensure that the specific requirements of the GCIMS are addressed and a recommendation will be presented to the GCIMS Steering committee for decision. Timeline: March 2005.

6.3.4 Data Quality

Criteria: The quality and integrity of application data should be monitored and maintained by data owners.
--

The quality and integrity of application data is monitored and maintained by the Programs that administer GCIMS, nevertheless, there are some outstanding issues regarding data completeness and accuracy. For example, pre-GCIMS payment information was found to exceed approved amounts in some cases. This issue exists because the “clean-up” of G&C data prior to GCIMS implementation has not been completed. Also, current payment data was often found to be out of sync with payment data in SAP. As a result, GCIMS users may not use payment information from GCIMS for corporate reporting purposes.



GCIMS has incorporated business rules, in the form of a series of input controls, to ensure that complete information is entered into the system. Data must be entered according to data validation rules for the purpose of project assessment. This process ensures that only those officers assigned to work on a given project have the authority to enter data related to that project (for related issues, see Section 6.3.3, above).

Systems controls in GCIMS are generally effective in processing transactions and ensuring data integrity, however, data integrity issues exist with respect to historical information. Specifically, some anomalies were noted with data prior to January 2000, where the paid amount exceeded the approved amount. These situations resulted when financial data was converted from other G&C systems without first validating the information. This issue has been identified in previous audit reports. In response, the GCIMS Transition Team has written electronic scripts to correct the problem. The time-frame for making these corrections in GCIMS was not identified as at March 31, 2003. The implications for G&C Programs are: accurate information may not be available for corporate reporting purposes; and accurate information may not be available in response to ATIP requests.

6.3.4.1 Recommendation

That the Director General, Financial Management Branch, in conjunction with the Chief Information Officer, Knowledge, Information and Technology Services and the respective G&C Program Directors, address the issues related to historical data in GCIMS.

6.3.4.1 Management Response

KITS would be pleased to assist FMB in any capacity with respect to data remediation but the direction for such resides outside of KITS.

FMB: The feasibility of meeting this requirement within GCIMS or through some other construct within PCH will need to be evaluated and discussed with all stakeholders within the context of an overall IM/IT strategy. Viable options if applicable to GCIMS, to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: March 2005.



We found payment information in GCIMS does not always reconcile to payment information in SAP. GCIMS and the SAP system are not integrated at this time. Payment information in GCIMS is currently updated through a nightly backfill process originating from SAP. In order to control the accuracy of data being transferred between systems, payment information must first be requested by an individual from the Program area who ensures that the payments are updated and correspond with the payment information in SAP. Payments between GCIMS and SAP may not reconcile if the following conditions exist: financial (allocation) coding does not match in GCIMS; the IFMS Commitment Number is not found in GCIMS; no corresponding payment is found in GCIMS; and the actual paid amount, backfilled from SAP into GCIMS, is different from the requested payment amount recorded in GCIMS.

G&C Program management do not have an effective regime for ensuring that grant and contribution payment information in GCIMS is reconciled to SAP on a regular basis. (6.3.4.1) Further, GCIMS users will often defer to SAP to obtain complete and accurate payment information for a given project or client, as payment data in GCIMS may not be up-to-date. (See 6.3.2.4, in Section 6.3.2) As a result, GCIMS reports that include payment data have limited use and, in some cases, could provide misleading information for management decision-making.

6.3.4.2 Recommendation

That the Financial Management Branch, with G&C Program Directors, develop a monitoring regime for ensuring that payment information is reconciled between GCIMS and SAP.

6.3.4.2 Management Response

This requirement has been identified as a priority and analysis of requirements and evaluation of options is underway. To date, we have conducted pilot testing of extended update capabilities to selected user fund centres and have embarked on ensuring that all program areas conduct a regular reconciliation of payment data using existing tools. Options to address this requirement will be reviewed and presented to the GCIMS Steering committee for decision as to relative importance and priority. Timeline: March 2005.