Science and Engineering Research Canada

NSERC CRSNG

AUDIT OF INFORMATION TECHNOLOGY

FINAL REPORT

Addressed to:

Natural Sciences and Engineering Research Council of Canada (NSERC)
Social Sciences and Humanities Research Council of Canada (SSHRC)

Presented by:

progestic international inc.

2650 Queensview, Suite 245
Ottawa, Ontario
K2B 8H6

January 27, 2005

Natural Sciences and Engineering Research Council of Canada
Conseil de recherches en sciences naturelles et en génie du Canada

Canada

TABLE OF CONTENTS

Description of tables:

1 EXECUTIVE SUMMARY

Introduction

Objectives - Two audit objectives were identified for the audit of Information Technology (IT).

1. Assess the Information Services Division (ISD) management control framework to ensure that the IT function is efficiently and effectively managed.
2. Review, examine, and assess the effectiveness of all ISD lines of services, IT operational activities, technological functions, and main processes.

Scope - The main focus of the audit was the ISD. The audit covered:

- The ISD management control framework, and
- All operational IT functions, services, processes, and activities.

Observations concerning the ISD management control framework

A formal IT governance structure is not in place in NSERC and SSHRC. Adopting a strategic approach to governing IT in NSERC and SSHRC will complement current ISD management practices and is necessary if both Councils are to achieve their business objectives. Some of the key issues missing in the current ISD governance framework are a governing body responsible to make strategic decisions for IT, the availability of an IT vision and a comprehensive IT plan, the accessibility to a comprehensive set of IT policies, the setting of service targets to measure ISD performance, and rigorous risk management practices.

As IT becomes increasingly crucial to the support, sustainability and growth of business, it is imperative for NSERC and SSHRC executive management to understand how to effectively measure IT performance. The responsibility to control the formulation and implementation of IT strategy to ensure the fusion of business and IT is called IT governance. The purpose of IT governance is to direct IT endeavours to ensure that ISD's performance meets the following objectives:

- IT is aligned with the Councils' businesses and realises the expected benefits,
- IT exploits opportunities and maximises benefits,
- IT resources are used responsibly, and
- IT risks are managed appropriately.

Areas of improvements – Several areas of improvements are required to ensure that the NSERC and SSHRC IT function provides all the expected benefits. Each area of improvements is specified in the next paragraphs along with our recommendation.

1. *An appropriate governance structure and process has not been developed to oversee the vision and strategic orientation for IT, review and approve IT policies, and set the priority of IT projects.* Our analysis led us to conclude that ISD does not have a formal discussion forum to share concerns with IT services, express satisfaction level with corporate applications and/or IT services, set priorities for IT projects, and participate in the strategic IT decisions.

We recommended that an Information Technology Steering Committee (ITSC) be established to connect end-users and senior management with the ISD organisation, oversee the strategic orientation and vision for IT by approving the IT plan, vision, and policies, appraise the viability and worth of IT projects to be undertaken, and recommend priorities and funding to the Management Committees.

2. *For the current fiscal year and past fiscal years ISD has not completed a comprehensive IT plan describing all its projects (system development, infrastructure, procurement, etc.). Furthermore, an IT vision has not been developed to identify the general technological directions ISD intends to follow in the next two to three years.* Each year, ISD produces an IT Plan based on the evolution of the core business applications (eBusiness, ESD, NAMIS, and AMIS). Even if the annual fiscal year budget process identifies and account for all IT projects, we noticed that the IT plan does not include all the infrastructure projects required to support the business projects or enhance the current network, office automation or telecommunication infrastructure.

We recommended that ISD produce a more comprehensive IT plan that will include all core business projects, ISD special projects (where applicable), office automation or infrastructure projects and that an IT technological vision covering the next two to three year be developed.

3. *ISD has not completed a threat and risk assessment (TRA) to determine the vulnerabilities associated to sensitive information, assets and employees and select risk-avoidance options to implement cost-effective safeguards.* While some TRAs were completed for selected system development projects, TRAs were not rigorously completed on all system development initiative and ISD operational activities to assess risks and vulnerabilities.

We recommended that ISD conduct a comprehensive TRA of its IT infrastructure environment.

4. *A comprehensive IT security plan has not yet been produced to justify, identify, prioritise, schedule, and estimate all IT security projects*. Our examination of current operations revealed that security projects take place each fiscal year. However, NSERC and SSHRC Management teams are not always aware of the overall costs and effort related to these security projects and do not currently participate in the establishment of priorities for each one.

We recommended that ISD articulate an IT security plan using the information contained in the Security Compendium document and the ISD-wide TRA exercise.

5. *ISD has not developed all necessary IT policies and standards to set the rules and regulations for the IT managerial, operational, and administrative frameworks*. ISD published few policies related to IT: the Acceptable Use of Electronic Network Policy, the Telework Policy, and the computer room access policy. Furthermore, ISD has not yet completed the development of its own IT security policy. Treasury Board Secretariat clearly states in its Management of Information Technology Standard (MITS) document that every federal organisation shall develop its own IT security policy based on the Government Security Policy.

We recommended that ISD identify the IT areas to be covered by IT policies and that a priority and a development schedule be assigned to each new policy.

6. *The document entitled "Service Level Agreement (SLA) between ISD, CASD, NSERC and SSHRC" dated March 2004 contains very few service targets leading to the measurement of ISD performance.* In March 2004, ISD reviewed and renegotiated its SLA with its three main user communities: CASD, NSERC and SSHRC. Our review of the SLA document revealed that in its current form, the SLA has not established service targets leading to the measurement of ISD performance.

   We recommended that ISD review its SLA and identify performance targets for Network Administration, System Development, Helpdesk Services, Internet and Intranet.

7. *The current Disaster Recovery Plan (DRP) document lacks operational details allowing a structured, orderly and timely recovery of IT operations.* Even if some security measures currently in place could be used to recover IT services, we concluded that should a major disaster strike the computer room, the continuation of IT operations could be compromised. Our analysis of the current DRP document led us to conclude that in its present state, the DRP does not contain all the essential procedures allowing a timely recovery of IT operations. Consequently, we concluded that should a disaster strike the computer room, the continuation of NSERC and SSHRC business operations is at risk.

   We recommended that the Security Steering Committee assign a timetable to update the DRP and that ISD review the existing DRP document.

Observations related to the ISD operational activities.

System development - *ISD uses several System Development Life Cycle (SDLC) and Project Management Frameworks during the development of NSERC and SSHRC core business applications. Our analysis led us to conclude that each SDLC provides good controls to develop, manage, track, test changes, and implement the applications.*

In any given year, several smaller system development initiatives are completed in addition to the development of the core application systems. Other system development projects sometimes classified as "special projects" respond to specific business needs or services such as the Intranet, Business Object reports, FDSR, Common CV, Family Album, IMEP, eCIMS, eScoring etc. Considering that ISD has not yet provided a definition to the term "special project", we described it as "*Special projects are system development projects that are either initiated by an ad-hoc user request or initiated and justified by ISD, not controlled by any user committee, and not following any particular SDLC".* Approximately 15 staff are involved supporting non-core application projects. However, it is important to note that many of these staff supporting special projects have other duties and the development and maintenance of special projects is only one of their responsibilities.

Our audit revealed that special projects are not developed and managed with the same rigour as system development related to core applications, that the IT plan does not yet describe or prioritizes these special projects, and their development processes do not follow any standard methodology.

We recommended that ISD
- Describe the term "special project",
- Where the scope warrants, describe and prioritise special projects in the IT plan,
- Ensure that a project plan is developed for each project, and
- Where the scope warrants, ensure that the development process follows a formal SDLC.

End users support services - *Nine ISD groups provide end user support services. All interviewees indicated that they were satisfied with services received from each group especially the ones provided by the ISD Helpdesk group responsible to support and manage the desktop environment (600 desktops and 100 printers) and provide office automation support services to NSERC and SSHRC users.*

Following our analysis we concluded that ISD does not capitalise on the benefits of using a single point of contact to provide end-user support services and capture information on each end user service request. Only two support groups (ISD Helpdesk and eBusiness Helpdesk) use the Remedy incident tracking system to record information on service requests. A formal escalation process has not been established to track problems until satisfactory resolution outside of the two aforementioned areas. We also noticed that insufficient information is captured in the Remedy database to measure ISD's performance related to end users support services.

Consequently, several recommendations were formulated. Three of these are:
- Investigate the advantages of creating a central focal point for all ISD support requests,
- Investigate the advantages of endorsing a more comprehensive incident tracking system, and
- Institute a formal escalation process to solve more complex problems.

Technical Services - *The Technical Support group manages the infrastructure environment adequately.* It maintains approximately 90 servers. Given the operational importance placed on operational servers, they are kept current and software licenses are adequately managed and properly inventoried. One of the major strengths of Technical Services is the implementation and maintenance of security measures to protect the data, the infrastructure, and the office automation environment.

We did observe that Technical Support group does not use rigorous processes to document and track the infrastructure changes, and then communicate these changes to users prior to implementation.

We recommended that Technical Support group implement more rigorous change management and release management processes to document changes to the infrastructure, and communicate the nature of the changes to users and provide them with information on the impact of the implementation.

2 INTRODUCTION

The audit objectives, scope and methodology are described in Appendices B1, B2 and B3 respectively.

A detailed description of the Information System Division (ISD) is provided in Appendix C. It includes information on the ISD budget, its clients and lines of services, its organizational structure, and the breakdown of staff and consultants between the six responsibility centres.

In Appendix D, we have included the difficulties of managing an IT organization in the Year 2005. The auditor's views and opinions are provided to explain:

- the increasing complexity of the Information Technology world,
- the increasing need for security measures, and
- the increasing pressures on an Information Technology Organisation.

3 GOVERNANCE FRAMEWORK

Introduction - Over the past decades, IT organisations have migrated from commodity service providers to a strategic partners. IT organisations are now viewed as a tool for increasing business growth rather than just an expense. The primary goal for IT governance is to assure that the investment in IT generates value while mitigating associated risks. This can be done by implementing an organisational structure with clear roles for the responsibility of information, business processes, applications, infrastructure, etc.

General observation – *A formal IT governance structure is not in place in NSERC and SSHRC. Adopting a strategic approach to governing IT in NSERC and SSHRC will complement current ISD management practices and is necessary if both Councils are to achieve their business objectives. Some of the key issues missing in the current ISD governance framework are a governing body responsible to make strategic decisions for IT, the availability of an IT vision and a comprehensive IT plan, the accessibility to a comprehensive set of IT policies, the setting of service targets to measure ISD performance, and rigorous risk management practices.*

3.1 Governance structure

Observation – An appropriate governance structure and process have not been developed to oversee the vision and strategic orientation for IT, review and approve IT policies, and set the priority of IT projects

Analysis – From our interviews, we have concluded that users do not have a formal comprehensive discussion forum to share concerns with IT services, express satisfaction level with corporate applications and/or IT services, set priorities for IT projects, and participate in the strategic IT decisions.

A more comprehensive IT governance process would ensure that users are more actively involved in the management of IT activities and actively participate in the development of its orientation. In many organisations, an ITSC (Information Technology Steering Committee) has been established to connect end-users with the IT organisation. With time, it has become the main communication medium allowing end-users and the IT organisation to formally exchange information relative to users' needs, priorities, and satisfaction levels. Furthermore, the ITSC would oversee the strategic orientation and vision for IT by approving the IT plan, vision, and policies, appraises the viability and worth of IT projects to be undertaken, and recommends priorities and funding to the Management Committees.

The main role that needs to be fulfilled by the ITSC relates to IT governance. Business and Administration representatives must be positioned to challenge the actions, proposals and decisions of ISD. The attributions related to this role entail making sure IT priorities are properly assigned, essential IT management activities are undertaken and IT projects progress according to plan and budgets.

The main objectives of an ITSC are to:

- Co-ordinate and monitor the development of strategic IT projects to ensure adherence to priorities, objectives and budgets approved in the IT Plan;

- Appraise the viability and worth of IT projects to be undertaken, and recommend priorities and funding to the Management Committees;
- Provide strategic planning direction for the exploitation of IT resources (link business strategy to IT strategy, set objectives); and
- Recommend to Management Committees the long range IT plan, budget and priorities, IT policies and standards.

Conclusion – In the absence of an ITSC there is no formal discussion forum to regroup NSERC and SSHRC senior management and discuss common IT issues, share concerns, exchange and communicate essential information on IT issues. In today's business environment, we strongly advocate the need of users to be actively involved in the management of IT activities and to participate in the development of technological orientations. The ITSC would serve as the "glue" that will connect and cement end-users and ISD. It is the main communication channel allowing end-users and ISD to exchange information relative to users' needs, priorities, and satisfaction levels.

Recommendation 1

1. An Information Technology Steering Committee (ITSC) should be established to connect end-users and senior management with the ISD organisation, oversee the strategic orientation and vision for IT by approving the IT plan, vision, and policies, appraise the viability and worth of IT projects to be undertaken, and recommend priorities and funding to the Management Committees.

2. Formal terms of reference (TOR) should be developed for the ITSC and describe the ITSC's goal, objectives and scope, deliverables, membership, responsibility, accountability and authority, reporting relationship, and frequency of meetings. Without TOR, our experience has shown that committees lack focus and are doomed to fail.

3.2 The IT plan and the IT vision

Observation –*For the current fiscal year and past fiscal years ISD has not completed a comprehensive IT plan describing all its projects (system development, infrastructure, procurement, etc.). Furthermore, an IT vision has not been developed to identify the general technological directions ISD intends to follow in the next two to three years.*

Current situation with the IT plan - Each year, ISD produces an IT Plan based on the evolution of the core business applications (eBusiness, ESD, NAMIS and AMIS). Even if the annual fiscal year budget process identified and account for all IT projects, we noticed that the IT plan does not include all the infrastructure projects required to support the business projects or enhance the current network, office automation or telecommunication infrastructure. On a yearly basis, the Technical Support group completes numerous infrastructure projects; however, the descriptions and justifications of these projects are not included in the IT plan and a priority was not assigned to each one.

Although the business applications are central to the expansion and growth of the Councils programs, the IT plan needs to address the improvement and the maintenance of the IT infrastructure.

For other system development projects, including the special projects [1] we observed that ISD does yet not have a systematic methodology to collect users' needs. Several special projects are conducted every year, representing projects that were identified over the years by ISD's management or communicated to ISD by users (for example: Family Album, IMEP, Intranet, etc.). We noticed that these projects had not been justified and included in the IT plan.

Consequently, the IT plan only contains business program projects that are identified and prioritised by committees addressing business requirements (e.g. eBusiness Steering Committee, ESD Steering Committee, NSERC NAMIS User Group (NUG), and AMIS User Requirements Group). In relation to infrastructure projects and special ISD projects, we noticed that these committees do not participate in the definition of their requirements or setting up of their priorities. However, we noticed that even if the infrastructure projects are not included in the IT plan, the ones that support the business projects endorse and follow the same priorities and are developed in parallel.

Current situation with the IT vision - ISD has not yet published and communicated a technological vision to lead its technical infrastructure [2]over the next two to three years. It is the auditor's opinion that ISD has the basic information to produce this technological vision. Based on the collection of users' needs and the market trends imposed by independent vendor suppliers, ISD would have many of the necessary elements to identify a short to medium term technological vision that could then be used to give direction to the IT plan. However, we are of the opinion that the absence of corresponding and necessary Council strategic business plans does not facilitate the development of an IT vision.

A technology vision statement will give a focal point from which ISD can form technology priorities and plans as well as indicate the overall technical directions for future system development initiatives. The statement, like a general organisational vision statement, will reflect a technological target for how things might look different in the future.

Ever changing technology - Over the years, ISD has evolved in response to the evolution of NSERC and SSHRC program delivery, service operations, and office automation requirements. ISD's staff composition changed, and its technology was adapted to keep pace with current market trends.

---

[1] **Definition of Special Projects** - ISD did not define what constitutes a "special project". For the purpose of this audit, we gave our own definition:
"Special projects are system development projects that are either initiated by an ad-hoc user request or initiated and justified by ISD, not controlled by any user committee, and not following any particular SDLC".

[2] **Definition of infrastructure** - For the purposes of this report we have defined the term infrastructure as follows: *"A technology infrastructure provides the means by which users can access the automated facilities available within NSERC and SSHRC and includes such aspects as network topology, cabling, computer operations, servers, personnel computers, remote access capabilities, and the support for these services."* In our view, an IT infrastructure must be able to provide a robust, reliable and maintainable environment that is easily accessible by its users and can be managed with relative ease.

Considering the anticipated projects facing ISD, it is crucial that the IT strategy changes in anticipation of the future work environment and complements business needs. ISD has undergone significant changes over the years, and more disruptive changes are coming. Our review of literature indicates that new technologies are constantly introduced to the marketplace. Many of them present a break with customary thinking (Internet, Blackberry, Virtual Private Network, firewalls, security zones and measures, etc.). Anticipating and adapting to discontinuities are critical challenges for IT planning. Without a comprehensive IT plan and IT technological vision, IT organisations that only address today's issues fall behind and eventually their technology does not adequately support the client's needs.

ISD, like many other federal organisations, approaches innovation with caution. Often ISD selects and adopts the use of new technology only after it has been proven and endorsed by like entities. This situation is mainly due to the economic necessity and the unwillingness to risk scarce resources, as well as the need to ensure that minimum disruptions are brought to the network thus ensuring that the network is stable and its availability is reliable.

Priorities of any IT organisation based on literature - Our review of literature found on the Internet shows that the new age of IT is characterised by three driving factors:

1. The building of an IT infrastructure (priority 1 and 2) for operating a more agile and responsive enterprise,
2. The provision of good services to the user community (priority 3), and
3. The delivery of business applications and services (priority 4) that transform enterprise operations and make possible new relations in the value chain, as well as new scopes of operation.

Table 1: "IT" DRIVING FACTORS

PRIORITY	DESCRIPTION	CURRENT STATUS
1	Provide automated tools (desktop and corporate application systems) to maintain an appropriate level of efficiency in business and program operations	Interviews with users indicated that ISD's performance over the years has been very good in relation to providing office automation tools and developing / supporting core applications.
2	Increase effectiveness by building an infrastructure that can be exploited later. One of the key architectural challenges facing ISD is the selection and management of appropriate strategic platforms. Lead technology by exploring newer available technological trends.	In the absence of published IT vision, NSERC and SSHRC do not have an understanding of what technology might be able to offer in the future. Consequently, system development projects cannot capitalise on the IT vision and develop their systems accordingly.
3	Be a service organisation that provides timely and adequate services (Helpdesk) to support business programs and operations	Users expressed their satisfaction level with the current helpdesk services.
4	Ensure that the business operations are well supported by business application systems and that systems are developed based on a thorough collection of users' needs.	Business needs leading to the development of new system development projects are assembled by Business representatives. However, ISD did not communicate its IT vision and strategic technological platforms so that business representatives take advantage of this technological orientation in the development of their new business systems.

Rationales to justify the development of a comprehensive IT plan and an IT vision – The development of an IT plan and IT vision are two of the most important components of IT governance. The IT vision should attempt to identify what the technology will be like for end-users in the near future and provide strategic technological directions that will guide the selection of new office automation products or provide a technical orientation for system development initiatives. Consequently, ISD must focus today on delivering tomorrow's products.

The IT plan on the other hand establishes a blueprint identifying the overall business strategy (mission, mandate, objectives, critical success factors, and constraints), defines business areas (groups of functions and the application systems they use), and proposes a technological target environment for ISD. The IT plan will be able to provide a service and customer oriented direction for the incorporation of technology as a key enabler of the business processes. In addition, it should allow for the communication of IT strategic direction, rationale and timetable, and the benefits of adopting them.

Conclusion – Our analysis led us to conclude that ISD does not have a published IT vision and a comprehensive IT planning process leading to the development of a global IT plan. In recent years, ISD spent six to eight million dollars on technology and as most organisations, NSERC and SSHRC expect to realise payback from their investments. Although efforts are made to keep IT serving business requirements, some expectations for additional requirements remained unaddressed such as need to develop or enhance its infrastructure based on a 2-3 year vision.

Recommendation 2 – ISD should
1. Produce an IT technological vision covering the next two to three years,
2. Produce a more comprehensive IT plan that will include all core business projects, ISD special projects (where applicable), office automation and infrastructure projects.

3.3 Risk management

Observation – *ISD has not completed a threat and risk assessment (TRA) to determine the vulnerabilities associated to sensitive information, assets and employees and select risk-avoidance options to implement cost-effective safeguards.*

The government security policies (GSP) related to TRA - The GSP states that the conduct of TRAs is the fundamental principle in assessing the need for security measures to protect sensitive information, assets and employees. The GSP requires that departments assess threats and risk to which sensitive information and assets and employees are exposed, select risk-avoidance options, implement cost-effective safeguards, and develop emergency and business resumption plans, as required. In addition, the government's risk management policy makes it incumbent on managers to be informed about the security threats, vulnerabilities, impacts and risks to which their business operations may be subject. The standard approach to assessing risk is the use of the Threat and Risk Assessment (TRA).

Finally, the Management of Information Technology Security (MITS) standard specifies that an initial TRA should be completed for each new project to identify IT security requirements.

Analysis of current situation - In ISD, all new information systems development projects are required to complete a TRA at various stages of development. While some TRAs were completed for selected system development projects, TRAs were not rigorously completed on all system development initiatives and ISD operational activities to assess risks and vulnerabilities.

When TRAs were completed, the recommendations included in the TRA were used by ISD groups to identify and select IT protection measures and control measures to reduce or eliminate risks in the application systems, business process or IT infrastructure environment.

Conclusion – In the absence of TRA for all ISD operational environments, it is difficult to assess whether sufficient safeguards exist to respond to a threat to the provision of IT services.

Given the difficulty of implementing cost-effective IT safeguards after a system has been deployed, fix an operational infrastructure component that was infiltrated, and because technologies and threats continuously change, ISD must address security and be proactive in its detection of threats and risks.

When properly implemented, the IT risk management process helps to ensure that appropriate protective measures are built in and not added through expensive modifications or support activities. The proactive process of completing TRAs also confirms the need for minimum safeguards and shows the need for additional types or levels of safeguards.

Recommendation 3 – ISD should
1. Conduct a comprehensive TRA of its IT infrastructure environment, and
2. Develop the necessary guidelines and control measures ensuring that TRAs are systematically and rigorously completed for every System Development initiative, including the development of non-core application projects.

3.4 IT security plan

Observation –*A comprehensive IT security plan has not yet been produced to justify, identify, prioritize, schedule, and estimate all IT security projects*.

Analysis – The Government Security Policy (GSP) states that an IT security plan shall be produced to justify, identify, prioritise and estimate each IT security project. Our examination of current operations revealed that security projects take place each fiscal year. However, NSERC and SSHRC Management teams are not always aware of the overall costs and effort related to these security projects and do not currently participate in the establishment of priorities for each one.

Using the recommendations reported in previous TRAs, audit reports, or security studies, a *Compendium of Security Requirements* document was produced in February 2003 to regroup and list all these security recommendations. More than 125 projects are listed, many of which are IT related. In the minutes of the November 6, 2003 Security Steering Committee meeting, four security projects were selected from the Compendium and identified as high priorities:

- Training and awareness,
- Policy (personnel, physical, IT, contract and information),
- Business Resumption Plan (BRP) including the Disaster Recovery Plan (DRP), and
- Organisational development.

Our review of the Compendium document indicates that it cannot be considered as a corporate security plan because projects included in the compendium are not the results of recent TRAs for the IT operational activities.

To keep track of projects completed to date, a C*ompendium of Security Requirements Accomplished To Date* document is maintained and provides the status of projects. The March 2004 update states the priority and risk level associated with each project.

Conclusion - In the absence of an integrated IT security plan, NSERC and SSHRC management teams are not fully aware of current risks and weaknesses, and cannot appropriately identify and prioritise security activities or initiatives, identify responsibilities, targets, deadline, and rationalise budget considerations that would normally flow from planning discussions. Security is no longer something that is to be taken lightly or as an afterthought. It must be planned well in advance, depending upon the requirements of the Councils, as the implementation tools may take time and considerable resources to implement.

Recommendation 4

1. ISD should articulate its IT security plan using the information contained in the Security Compendium document and the ISD-wide TRA exercise recommended in chapter 3.3 – Risk Management.

3.5 IT policies and standards

Observation – *ISD has not developed all necessary IT policies and standards to set the rules and regulations for the IT managerial, operational, and administrative frameworks*.

Introduction - IT policies and standards, like the IT plan, are major components of the IT governance function. Policies and standards are difficult to identify, and are even harder to enforce. As technology becomes more and more complex, both grow increasingly important.

General IT policies - Through policies, an organization sets the rules and regulations for the IT framework. Our review of the current approved policies indicated that ISD published few policies related to IT: the Acceptable Use of Electronic Network Policy, the Telework policy, and the computer room access policy.

As no policies currently exist in IT areas, ISD managers and staff are without guidance and adopt what appears to be the best approach to serve their purpose. One of the examples supporting this statement is the presence of multiple system development life cycle methodologies.

IT security policies – We noted that even if ISD endorsed and complied with many operational standards included in the Treasury Board Secretariat (TBS) Government Security Policy (GSP) and the Management of Information Technology Security standard (MITS), it did not yet completed the development of its own IT security policy. The TBS MITS standard clearly states that every federal organisation must have its own IT security policy based on the GSP standard.

Many subjects need to be covered by specific IT security policies such as security of information, Personnel security, Physical security, Access control, and e-Mail management, infrastructure, etc. We understand that some of these components are the primary responsibility of the Administration Division (i.e. Physical security, Information Management including mail management, Personnel Security). However they need to be referenced in an IT security policy.

Standards - ISD has been successful in endorsing and enforcing the use of formal IT hardware and office automation software standards. Some of the most important are the MS Office Automation software suite, Windows 2000 Operating System, the IBM hardware platform for PCs and servers, and the microcomputer configuration standards applicable to all new PCs. Standards were also developed for e-mail, cabling, telecommunication, firewall, and virus protection.

The benefits can be seen today as the same standardized brand name computers or servers make the operational support much easier. As such, this standard combination allows for future expansion, allows for easier connectivity and inter-operationality of applications, and interfaces tools, and contributes to the stability of the current IT environment.

Recommendation 5

1. In collaboration with the Administration Division, ISD should identify the IT areas to be covered by IT policies, assign a priority and a development schedule to each new policy, develop each one according to the established timeline, present them to the IT steering committee for approval, and develop a roll out strategy to cover the communication to staff and posting on the Intranet.

3.6 The Service Level Agreement

Observation - *The document entitled "Service Level Agreement (SLA) between ISD, CASD, NSERC and SSHRC" dated March 2004 contains very few service targets leading to the measurement of ISD performance.*

Analysis of the SLA document - In March 2004, ISD reviewed and renegotiated its SLA with its three main user communities: CASD, NSERC and SSHRC. Our review of the SLA document revealed that in its current form, the SLA has not established service targets leading to the measurement of ISD performance.

Performance targets are normally used as a base for monitoring the quality of services and indicate the maximum allowable time for service delivery. They can be set for network accessibility, server or PC crash, server file backup, files restore from backup, setup of workstations, user-id creation, new hardware or software install, and many more

Our analysis revealed for priority 1, 2 and 3 problems, the SLA does not provide any resolution time. It only specifies a maximum time period to begin resolution. For the last 4 priorities levels (4, 5, 6, and 7) a maximum time period is specified to complete resolution. Furthermore, the SLA does not contain a list of hardware or software that will be supported by the ISD Help Desk (HD) and does not specify the escalation process required to promote effective, as well as timely management and resolution of support incidents. Escalation is a defined process in which a request for support service has reached its predetermined escalation threshold. It allows the Service Provider to raise priorities and add resources if and when required.

Monitoring the SLA –The SLA does not contain the reporting requirements to assess ISD performance. Not only should the SLA contain performance targets for several ISD services, but it should also contain the requirements (content and frequency) of reports that will highlight the measurement of each service target.

Conclusion – There is a need to guarantee that ISD services provided to end-users (Helpdesk, Network Operations, System Development, and other ISD activities such as Internet, Intranet) will be of high quality and meet pre-established and negotiated service level targets.

In its current state, the SLA does not constitute a binding document creating an accountability framework for end-user support services provided by the various helpdesk groups. Well-structured SLAs warrant performance targets and draft terms and conditions of the support services to be provided by the Service Provider (ISD).

We consider the SLA as an important part of the IT governance framework and of the end-user support structure. Not only must it be established, but it must also be strictly monitored and adhered to if the service support structure is to succeed.

The SLA must be meaningful and become part of an actual contract between the Service Provider (ISD) and the Service Recipients (Clients). This contractual agreement should formally define the rights of clients and the obligations of ISD. Typical elements of SLAs include network response time goals, repair time objectives, network availability targets, audit and reporting specifications procedures, definition and description of escalation process, definition of types of services provided, definition of service exclusions, and the description of roles and responsibilities or parties involved.

Recommendation 6

1. ISD should review its SLA and identify performance targets for Network Administration, System Development, Helpdesk Services, Internet and Intranet. These performance targets need to be negotiated with the clients, included in a revised SLA, monitored for compliance, reported on a regular basis, and communicated to the IT Steering Committee.

3.7 Disaster recovery plan (DRP)

Observation – *The current Disaster Recovery Plan (DRP) document lacks operational details allowing a structured, orderly and timely recovery of IT operations. Even if some security measures currently in place could be used to recover IT services, we concluded that should a major disaster strike the computer room, the continuation of IT operations could be compromised.*

Analysis - The primary purpose of a Disaster Recovery Plan (DRP) is to provide for the protection and restoration of IT facilities and capabilities, and to reduce the damaging consequences of any unexpected or undesirable event.

Federal government policy requires departments and agencies to establish a DRP to provide for the continued availability of critical services and assets. The program must include a governance structure, monitoring of overall readiness and continuous review, testing and audit of the program.

The Security Steering Committee has identified four main security priorities. One of them is the development of the Business Continuity Plan (BCP). The DRP is a sub-component of the BCP. Our review of the current project status indicates that the Security Working Group Committee is in the process of establishing an inventory of essential services, programs and operations, developing a list of equipment that could be shared with other organizations. In addition, we noticed that a specific timetable was not identified for this project and that an ISD staff was not dedicated to its development. Consequently, the project is progressing slowly.

Our analysis of the current DRP document led us to conclude that in its present state, the DRP does not contain all the essential procedures allowing a timely recovery of IT operations.
Our analysis of the current ISD DRP document led us to conclude that in its present state, the DRP provides NSERC and SSHRC authorities with a false sense of security because many important pieces of information have not been included in the plan, such as:

- An internal communication section describing the sequence of events and authority to initiate the plan,
- A section describing the activities to mobilise the disaster recovery team (the notification structure),
- A high level description of the sequence of events required to recover the IT operations in the shortest possible time,

- The groups responsible to reconstruct the paper files and to find the alternate locations to conduct application reviews are not clear,
- And the high level description of roles and responsibilities of each member of the Crisis Response Team.

We confirmed that many current operational security measures could be used in case of emergency to assist in the recovery of IT operations: backup practices, documentation of some server configurations, and outside storage are three of them.

Conclusion – In the absence of a well-articulated and comprehensive DRP, we conclude that IT operations would be seriously compromised should a major disaster strike the computer room. Consequently, the continuation of business operations would also be compromised.
Should ISD be forced into an unforeseen situation where the DRP would need to be activated, we have some reservations and doubts that, in its present form, the activation of the plan could provide all the expected outcomes and likely benefits in the shortest lapse of time.

Should NSERC and SSHRC wish to reduce its risks and ensure that the shortest recovery time is targeted for IT recovery, then the current DRP needs to be reviewed and be more comprehensive.

Recommendation 7

1. The Security Steering Committee should assign a timetable to update the DRP.
2. The Director ISD should formally assign the responsibility to review the existing DRP document to one of his managers.

4 END-USERS SUPPORT MANAGEMENT

Observations – *ISD does not capitalize on the benefits of a centralized organization providing a single point of contact for end-users. Nine ISD groups currently provide end user support services. Only two of them use the Remedy incident tracking system to record information about their service requests. A limited functionality version of the Remedy software was purchased and led to the internal development of several ticket recording interfaces. A formal escalation system has not been established to track problems until satisfactory resolution outside the aforementioned areas. Since service targets have not been developed in the SLA, little information is captured in the Remedy database to ISD's measure performance. Performance reporting and incident trend analyses are not occurring.*

The ISD Helpdesk (HD) group provides end-users support services (mainly office automation related) to both Councils' internal users. Users contact ISD HD directly by phone, e-mail or by walking to the front service desk. Some of the services provided are in support of desktop hardware and office automation software. The HD controls all acquisitions of hardware and software except for the ones related to the infrastructure (servers, hubs, routers, switches, etc.) and corporate software licenses.

The HD is the primary point of contact for internal clients (NSERC and SSHRC), corporate users, regional staff, teleworkers, and remote workers. It is composed of two distinct support groups:

- The HD group (4 staff) provides the 1st and 2nd level support (95% resolution), and
- The IT analysts (ITA) (4 staff) provide one of the 3rd level support groups that will resolve the remaining 5% support requests for Office Automation (OA) Microsoft suite, DB access, MS software, and write scripts and macros for users.

Over the last few years, the need for end-user support services has significantly increased. There are several causes for this workload increase such as increasing number of workstations (approximately 600) and printers (approximately 100), support of PCs at home, support of teleworkers (14), significant number of Office Automation Software (approximately 175), increase number of laptops (125), support for remote access, large number of additional hardware (7 scanners, 15 projectors and approximately 150 PDAs) and acquisition and configuration of hardware.

Comments received from interviews were unanimous: NSERC and SSHRC's users spoke highly of the ISD Helpdesk. They mentioned that staff have a good technical background, good telephone skills in dealing with distraught people, have good communication skills, and are pleasant, friendly and patient in nature. They also mentioned that problems are solved rapidly.

The eBusiness – ESD Helpdesk group provides end-users support services (mainly on-line application systems) to NSERC eBusiness application users, SSHRC ESD online application users, and NSERC or SSHRC program people. Users contact them directly by phone or e-mail. It is the primary point of contact for external NSERC and SSHRC clients.

On a regular basis, the group is composed of two staff and consultants. As of December 1, there were 3 consultants. During the peak period (grant application period), additional consultants are hired to assist and cover a longer daily support period.
Workload fluctuates monthly and follows the impact of the life cycle associated to each contribution program. Over the last few years, the need for end-user support services has significantly increased. Some of the main causes are the increased number of external clients caused by an increase number of grant programs, the continual addition of new services, and the increased functionality in the core applications.

Some volumetric statistics are posted on the Intranet site and clearly demonstrate this increase in workload. For instance in 2002, 10,097 support requests were received. The number skyrocketed to 25,503 in 2003. From January to August 2004, the total of support requests was already totalling 7,700. It is anticipated that the total number of support requests could well exceed 20,000 calls considering the peak period of August to December peak period.

No external clients were interviewed during our audit. Our analysis of the quality of services was based on the feedback received from Program people, representatives from the eCentre, and testimonial e-mails received from external clients. Based on this information we concluded that service recipients are satisfied with services received.

Several other support groups provide end user support services:

- the NAMIS and AMIS support groups provide functional support for the core business applications,
- the NAMIS and AMIS Data Administration groups provide database support to the two System Development groups, the Database Administration group, and Program people,
- the Database Administration group provides database support for all core application systems to the two System Development groups, the Data Administration groups, as well as Program people, and
- the Intranet support group provides support for the Intranet.

The support requests originate from an e-mail hotline address, telephone, or a Remedy ticket sent by the ISD or eBusiness Helpdesk groups. It is important to mention that staff providing these support services are not exclusively dedicated to these duties. Support services are only one of their main areas of responsibilities.

Support requests originating from an e-mail or a telephone conversation are not logged in the Remedy system. Consequently, there are no volumetric statistics available, only estimates. For instance, the SSHRC AMIS Quality Assurance group estimated that approximately 100 support requests are received every month, but this is only an estimate. Interviews with staff providing these support services revealed that these support services are distracting them from their main duties; as such, staff reported that support activities were very time consuming especially during peak periods.

Limits of the current Remedy incident tracking system – The ISD HD and eBusiness – ESD HD are the only two support groups that use and record their support requests in the Remedy system. This incident tracking system is one of the best on the market and is widely used by

other federal IT organisations. However, because ISD only purchased a "shell" version of the Remedy system, its functionality and user interfaces have been developed in-house.

Our review of the system revealed many of its limits. Furthermore, the current version of the Remedy system does not provide a reporting capacity. This function was also developed in house and produces reports that are based on the limited data that was captured and documented for every incident.

Since the system only registers partial incident or resolution information, statistics, performance information, and trend analysis are also limited. To produce such information, additional data needs to be captured and registered for each support request. Consequently, we conclude that since the current Remedy system contains limited functionality, it limits the production of precise statistical information.

Observed weaknesses in the escalation process – When necessary, HD staff escalate the support requests to other groups. This escalation process has not been formally described and included in the SLA. Comprehensive SLAs generally specify the timely conditions surrounding the escalation process. While it can be difficult for the HD's to "pressure" other groups to complete their tickets, HD's do not close tickets until they are satisfactorily resolved.

For instance, the ISD HD and the eBusiness – ESD HD are the first line of contact for support services for their respective users. Currently, neither group is the "owner" of the incidents nor has any support groups been made accountable for the successful resolution of every incident or the resolution of the incident in a timely fashion. It is our opinion that current incident management processes do not track the reported support requests until satisfactory resolution. When HD staff cannot resolve the problem, the Remedy ticket is "transferred" to a new support group and neither HD groups were given the accountability to track the problem until complete resolution. Overdue tickets are escalated to the manager of the ISD HD for follow up. The ESD HD does close the ticket once the problem is resolved.

Measuring results and reporting performance – ISD did not put in place a performance measurement framework to measure the results of its Helpdesk services. Very little statistics, performance results, or trend analyses are produced and communicated to users. Some general statistics are produced but not officially published. The SLA does not specify that performance be measured and that reports will be produced and published.

Measuring user satisfaction – ISD did not put in place a formal system to collect user satisfaction. We were informed that ISD's NSERC eBus. team did propose a formal mechanism to collect client satisfaction on the services provided; however this mechanism was not implemented because the eCentre group was conducting a Service Improvement Initiative (SII) analysis on behalf of NSERC. Currently, the user satisfaction is mainly evaluated by comments included in e-mails, or face to face discussions with users.

Conclusion - ISD does not capitalize on the benefits of a centralized organization providing a single point of contact for end-users. A central Helpdesk would have the capability to log all incoming calls, track all problems from the initial call through to completion, provide quicker resolution of problems, rapid scheduling and dispatching of support staff, provide a more efficient use of ISD skilled and specialized resources, and produce performance reporting and statistics for all ISD end user support function.

Creating a first-class Helpdesk function is imperative. The functionality or dysfunctionality of the HelpDesk services is one of the main factors establishing ISD's reputation. While a strong technical support process ensures that ISD is viewed as a solid, competent organization, a weak technical support process may serve to undermine all other ISD initiatives to build its reputation.

Recommendations 8 - ISD should

1. Investigate the advantages of creating a central focal point for all ISD support requests,
2. Investigate the advantages of endorsing a more comprehensive incident tracking system and maintaining a single database for all service requests,
3. Institute a formal escalation process to solve more complex problems,
4. Review the accountability of the ISD HD and the eBusiness – ESD HD groups to ensure that each group becomes accountable to track and monitor the escalated problems until full resolution,
5. Monitor the performance targets specified in the SLA, and
6. Ensure that performance reports are produced to measure the attainments of objectives stated in the SLA.

5 MANAGEMENT OF INFRASTRUCTURE

5.1 Management of ISD Infrastructure [3]

Observation – *The Technical Services group manages the infrastructure environment adequately*.

Current technology - Over the years, ISD followed the trends and evolutions of technology imposed by independent vendors. As such, it frequently upgraded its hardware and software standards to keep pace with technology trends. A quick review of the ISD technological environment revealed that its technological environment is not only complex; it is also diversified.

Servers – ISD maintains approximately 90 servers. Servers are used to host NSERC and SSHRC numerous development, test or production environment for specific corporate applications and databases, and control various infrastructure functions such as firewalls, remote access, Internet and Intranet, e-mail, printer management, etc.

Several reasons can be invoked to justify the need to maintain this large portfolio of servers. ISD supports two independent Councils where each one wishes to maintain a separate and independent technological environment. Furthermore, for security reasons, ISD maintains three distinct environments for corporate applications (system development, testing environment, and production environment) and distinct environments for domain servers (primary and backup), mail controllers, Internet, etc. The existing server hardware appears to be efficient in terms of providing service to the end-user community. Given the operational importance placed on operational servers, the Technical Support group is very conscious of this fact and ensures that servers are kept current, with a turnover approximately every three to four years to ensure continued and non-disruptive operation.

Operating System (OS) for servers – The Technical Support group standardized the Operating System (OS). Two distinct OS are used to manage servers: Windows 2000, and Windows 2000 Advanced. The Windows NT4 OS is only used to manage the Human Resources Information System (HRIS). We observed that each one has been updated with the latest updates provided by the Software vendors.

Operating Systems (OS) for desktop and laptops – Windows 2000 Professional has been selected as the standard OS for PCs and Laptops. Similarly to any other OS, the software needs to be updated with patches sent by Microsoft. Currently, the OS update process is done manually. ISD Helpdesk personnel need to physically visit every workstation to update it on-site. Not only this is a tedious task, but it consumes time. Consequently, the desktop OS is not maintained with the same rigour as the OS for servers.

[3] Infrastructure – The definition of the term "infrastructure" is provided in chapter 3.2

PC hardware platform – For desktop PCs, ISD endorsed the IBM PC as its hardware standard. Each year, prior to purchasing the new desktop, the desktop technical standards (processor, RAM, Video card, Monitor, Network Interface Card (NIC), Hard drive) are revisited to ensure that ISD will adhere and follow market trends. As such, the current desktop hardware meets or exceeds the minimum requirements for Windows 2000 Professional OS.

Office Automation (OA) software - More than 175 software applications are maintained by ISD. Some software applications are only one-of (such as Auto-Cad, CorelDraw, etc.) while others are licensed software used for Office automation (MicroSoft suite, Adobe, Acrobat, MS Exchange, Outlook), Internet and Intranet (Netscape, Internet Explorer, DreamWeaver), System Development activities (SQL, Sybase, Rational Clearquest, MS Project, Java, Crystal Reports, FoxPro, Free Balance,), Helpdesk operations (Remedy), PDA (Palm desktop), Palm500, Security (Entrust), Desktop management (Windows XP), network management (Windows NT), etc.

Our audit revealed that ISD manages its licenses adequately and maintains an accurate inventory of its office automation software and licences.

Software Update Services (SUS) - ISD is well aware of the fact that processes used to update the desktop OS could be improved. Consequently, Technical Support is currently testing the Microsoft Software Update Services (SUS) product, a free patch management tool to help Network Administrators deploy patches to the desktop OS more easily. Today the ISD Technical Support group has to frequently check the Microsoft Windows Update site or the Microsoft Security Web site for new patches. If present, it has to manually download each patch that has been made available since it last visited the site. Then it will test the patches and then distribute them manually or by using their traditional software-distribution tools.

Should ISD adhere to SUS, the process would become more foolproof. SUS provides dynamic notification of critical updates to Windows computers as well as automatic distribution of those updates to the desktops and servers OS. Consequently, Microsoft SUS gives the Network Administrator control over updates since the Administrator can test and approve updates from the public Windows Update site before deployment.

The Technical Support group plans to implement this software by the end of 2004. Once implemented, it will facilitate the roll out of updates to the desktop OS.

Systems Management Server (SMS) – SMS provides a comprehensive solution for change and configuration management for the ISD platform enabling ISD to provide relevant software and updates to users quickly and cost-effectively. When integrated with SUS, SMS becomes a very good tool to deploy patches to servers. SMS is a very powerful tool for the Network Administrator. It contains functionality for detailed hardware and software inventories and metering, software distribution and installation, and remote troubleshooting tools.

Conclusion – The Technical Support group has a complex, diversified infrastructure environment to manage. Considering the significant amount of equipment to manage, we concluded that the equipment is well maintained and the Operating Systems have been updated with the most current software patches.

Suggestion - We suggest that ISD reviews the use of the SMS software within ISD as we consider that its functionality is not used at its full capacity.

5.2 Security of infrastructure

Observation - *Our review of operational security measures indicates that adequate detection and protection measures have been implemented in the infrastructure and comply with the GSP.*

Responsibility for IT security within ISD – The Technical Support group is responsible for IT security including the testing and installation of the OS security patches. The Technical Support group is alert to the fact that the Internet has drastically increased vulnerability. It has been proactive in implementing adequate counter measures against new cyber threats. IT security is a constant preoccupation for the Technical Support group. Over the years, it implemented several advanced security measures to protect the network, systems and data against loss, destruction, unauthorised access, viruses, etc. Such security includes firewalls, content filtering gateways, anti-virus software for servers and the PCs, detection of SPAM, and an intrusion detection system (Internet Security System software (ISS)) for the Internet.

Our review of operational security measures indicates that adequate detection and protection measures have been implemented in the infrastructure and comply with the GSP. These examples are:

- physical security measures provide good access control to the ISD work space and the computer room,
- inventories of IT assets and licenses are kept current,
- processes to dispose of older hardware comply with the GSP,
- IMEP (Intake-Modification-Exit Process) system is used to manage security events surrounding the movement of staff,
- network security measures provided by Firewall, Virus detection software, and SPAM detection software are adequate,
- security measures for remote access provide good control measures,
- backup measures are adequate,
- controls surrounding the management of IP addresses are adequate, and
- monitoring practices surrounding the infrastructure environment are adequate.

5.3 Change management and release management

Observation - *Technical Support does not use rigorous processes to document and track the infrastructure changes and then communicate these changes to users prior to implementation.*

Change management is defined as the process that controls changes to all infrastructure configuration items, within the live environment. It is not responsible for controlling the changes within ongoing system development projects which are controlled by the project change process.

Status - Technical Support does not apply rigorous processes (similar to Rational Clear Quest) to document and track its changes to the infrastructure (hardware or software). Most of the infrastructure changes originate from patches supplied by software vendors. Some patches are for the OS (servers or desktop), or software that manages the firewall, viruses, office automation, etc. As such, Technical Support reviews the changes included in the Software Patches sent by the suppliers and decides which changes need to be implemented in the ISD technical environment.

We understand Technical Support needs to address urgent situations frequently. It needs to react to emergency situation compromising the performance or availability or the infrastructure. As such, when an urgent situation arises, a fast tracking process needs to be followed, and changes that were incorporated in the technical environment are more difficult to document. However, this should only be viewed as an optional route to faster implementation since it carries considerably greater risks than the normal change process procedure. This urgent process should typically be used for emergency problem resolution.

Release management – definition – It is the process that coordinates the many activities involved with the release of hardware (new or enhancements), Operating system or Office automation software (new or enhancements) and associated documentation and communication processes across the client's environment.

Status - Several interviewees (representatives from ISD, Service, and Program) mentioned that they were not satisfied with the level of details communicated to them prior to the implementation of a change to an infrastructure component. They mentioned that on several occasions impacts associated to the nature of the changes were not communicated prior to roll out. For instance, we consider that it is not sufficient to inform users that "maintenance will be performed on the firewall". Some users, such as selected ISD groups (i.e. HD and System Development groups) should receive additional information on the nature of the changes and the impact should be communicated to them. In the absence of an efficient release management process, the ISD Helpdesk is often confronted with users' calls reporting a potential problem necessitating investigation.

Pressure on the Helpdesk groups - One of the responsibilities of the HelpDesk groups is to follow the evolution of the IT infrastructure and business applications. As improvements / changes to the operational environment occur (IT infrastructure or business applications), the change management and release management processes must ensure that Helpdesk organizations are well-informed of changes so that they are able to provide end-user support and are knowledgeable of this new support environment. As business pressures mount, end-users become more demanding. It then becomes more important to answer or "close / solve" as many support requests as possible on the first support call. This will not only improve the efficiency of the HelpDesk services but will also contribute to an increase in end-users' satisfaction.

Recommendation 9

1. Technical Support group should implement more rigorous change management and release management processes to document changes to the infrastructure, and communicate the nature of the changes to users and provide users with information on the impact of the implementation.

6 SYSTEM DEVELOPMENT

6.1 Special projects[4]

Observation – S*pecial projects are not developed and managed with the same rigour as system development related to core applications. Their descriptions and priorities are not included in the yearly IT plan and the system development processes does not follow a standard methodology.*

Impact of special projects on ISD - In any given year, several smaller system initiatives are developed in addition to system development initiatives related to core applications. These other system development projects called "special projects" dealt with Intranet, Business Object reports, FDSR, Common CV, Common Grant System, Family Album, IMEP, ECIMS, eScoring, and many more.

Approximately 15 staff are involved in their developments. It is however important to note that many of these staff have other duties and the development and maintenance of special projects is only one of their responsibilities.

Table 2: IDENTIFICATION OF STAFF INVOLVED IN THE DEVELOPMENT OF SPECIAL PROJECTS

ISD GROUPS	TOTAL	MANAGERS AND STAFF	CONSULTANTS
TS - Special projects	4	3	1
DA - Intranet Group	3	1	2
HD - Information Technology Analysts	4	4	0
SD1 - System development – Business Intelligence	4	3	1
TOTAL SPECIAL PROJECTS	**15**	**11**	**4**

Examples of special projects - One of the special projects ISD is currently facing is the conversion of the ESD online application. This system was initially written using the Power Builder software language. Considering that this software is no longer supported by the supplier, the system needs to be converted using a new software language. This conversion project could be initiated as early as December 2004. At the end of October 2004, a project plan covering the nature of the project (description of the overall project, description and selection of the new software, staffing strategy, estimated costs and schedule) had not yet been produced.

The Intranet is also another special project. The first generation of the Intranet was the result of a pilot project ISD undertook to introduce an internal communication tool to both Councils. In particular, the pilot was used to disseminate CASD information. It was designed with the assistance of representatives from CASD and used ideas obtained from Intranets in various other government departments. There was little participation from non-CASD staff and user requirements were not documented.

[4] The definition of the term "special projects" is provided in chapter 3.2

As part of the implementation of the production Intranet, a survey of NSERC and SSHRC's staff was conducted to obtain feedback on the pilot; TBS look and feel standards were followed, and workshops were held with staff to design the navigation. Also, a governance body, the Intranet Committee (ICom), was established, with representatives from both Councils, to make decisions concerning policies, design, standards and procedures.

Despite this, users still found that the structure of the production Intranet was complex; the navigation was not intuitive and difficult, and the search function that came with the tool contained little functionality. In summary, the Intranet was not a user friendly system. ISD was well aware that in its current form, NSERC and SSHRC's users found little benefit for its use other than for HR related information. To help address these issues and obtain more user input, an Intranet Editors' User Group, consisting of approximately 100 editors from both Councils, was formed last summer and a formal survey of all staff is planned for the new year.

Conclusion - Special Projects are an intrinsic part of ISD yearly workload. In any given year, they consume and will continue to consume many resources. Their developments follow no formal SDLC, are developed with less rigour than regular system development initiatives, and are not included in the IT plan.

Recommendation 10 – ISD should
1. Describe the term "special project",
2. Where the scope warrants, describe and prioritise special projects in the IT plan.
3. Ensure that a project plan is developed for each project, and
4. Where the scope warrants, ensure that the development process follows a formal SDLC.

6.2 System development and maintenance for core applications

Observation – *The System Development Life Cycle and Project Management Framework vary for each core application. Our analysis led us to conclude that each one provides good controls to develop, manage and track changes, test changes, and roll out the applications.*

The system development function - Two distinct groups provide system development and maintenance for corporate applications:

- **The NSERC eBusiness System Development (SD) group** – This group deals exclusively with the development of NSERC eBusiness projects and the maintenance of the NSERC online application. The eBusiness Steering Committee identifies, sets priorities, and communicates the projects to ISD. The current IT plan includes these projects. The group is composed of 6 staff and 5 consultants.

  The eCentre group (program organisation) is responsible to produce the user requirements, and manage the projects. The ISD eBusiness SD group is responsible to complement the user requirements to produce the functional specifications, develop, test, and roll out the new system.

Once in operations, the ISD Technical Support group is responsible to ensure the availability of servers and maintain security measures for the network, while the SD group is responsible for its performance.

- **The Corporate Application System Development (SD) group** – This SD group maintains several core applications (AMIS, ESD online, NAMIS, FPAM, SMS, HRIS, for several clients (SSHRC, NSERC and CASD Directorates).

The distribution of staff is as follows:

Table 3: Corporate Application System Development Groups	**TOTAL**	**MANAGERS AND STAFF**	**CONSULTANTS**
NSERC – NAMIS - System Development and maintenance	7	3	4
SSHRC – AMIS – System Development and maintenance	7	5	2
SSHRC – ESD - System development and maintenance	4	2	2
TOTAL	**18**	**10**	**8**

System Development Life Cycle (SDLC) and Project Management Framework - Within ISD, each core application system development and maintenance activities follow a different SDLC and Project Management framework. We also noticed that different change management and release management processes existed. Even if these methodologies and processes differ for each core application, our analysis led us to conclude that each one provides good controls to develop, manage and track changes, test changes, and roll out the applications.

APPENDIX A: SUMMARY OF RECOMMENDATIONS

#	PRIORITY	DESCRIPTION
Ref: Chapter 3.1		**GOVERNANCE FRAMEWORK – Information Technology Steering Committee**
1.1	HIGH	An Information Technology Steering Committee (ITSC) should be established to connect end-users and senior management with the ISD organisation, oversee the strategic orientation and vision for IT by approving the IT plan, vision, and policies, appraise the viability and worth of IT projects to be undertaken, and recommend priorities and funding to the Management Committees.
1.2	HIGH	Formal terms of reference (TOR) should be developed for the ITSC and describe the ITSC's goal, objectives and scope, deliverables, membership, responsibility, accountability and authority, reporting relationship, and frequency of meetings. Without TOR, our experience has shown that committees lack focus and are doomed to fail.
Ref: Chapter 3.2		**GOVERNANCE FRAMEWORK – The IT plan and the IT vision**
2.1	HIGH	Produce an IT technological vision covering the next two to three years.
2.2	HIGH	ISD should produce a more comprehensive IT plan that will include all core business projects, ISD special projects (where applicable), office automation and infrastructure projects.
Ref: Chapter 3.3		**GOVERNANCE FRAMEWORK – Risk management**
3.1	MEDIUM	ISD should conduct a comprehensive TRA of its IT infrastructure environment.
3.2	MEDIUM	ISD should develop the necessary guidelines and control measures ensuring that TRAs are systematically and rigorously completed for every System Development initiative, including the development of non-core application projects.

#	PRIORITY	DESCRIPTION
Ref: Chapter 3.4		**GOVERNANCE FRAMEWORK – IT security plan**
4.1	LOW	ISD should articulate its IT security plan using the information contained in the Security Compendium document and the ISD-wide TRA exercise recommended in chapter 3.3 – Risk Management
Ref: Chapter 3.5		**GOVERNANCE FRAMEWORK – IT policies and standards**
5.1	MEDIUM	In collaboration with the Administration Division, ISD should identify the IT areas to be covered by IT policies, assign a priority and a development schedule to each new policy, develop each one according to the established timeline, present them to the IT steering committee for approval, and develop a roll out strategy to cover the communication to staff and posting on the Intranet.
Ref: Chapter 3.6		**GOVERNANCE FRAMEWORK – The service level agreement (SLA)**
6.1	HIGH	ISD should review its SLA and identify performance targets for Network Administration, System Development, Helpdesk Services, Internet and Intranet. These performance targets need to be negotiated with the clients, included in a revised SLA, monitored for compliance, reported on a regular basis, and communicated to the IT Steering Committee.
Ref: Chapter 3.7		**GOVERNANCE FRAMEWORK – Disaster recovery plan (DRP)**
7.1	HIGH	The Security Steering Committee should assign a timetable to update the DRP.
7.2	MEDIUM	The Director ISD should formally assign the responsibility to review the existing DRP document to one of his managers.
Ref: Chapter 4		**END USERS SUPPORT MANAGEMENT**
8.1	LOW	ISD should investigate the advantages of creating a central focal point for all ISD support requests.

#	PRIORITY	DESCRIPTION
8.2	MEDIUM	ISD should investigate the advantages of endorsing a more comprehensive incident tracking system and maintaining a single database for all service requests.
8.3	MEDIUM	ISD should institute a formal escalation process to solve more complex problems.
8.4	MEDIUM	ISD should review the accountability of the ISD HD and the eBusiness – ESD HD groups to ensure that each group becomes accountable to track and monitor the escalated problems until full resolution.
8.5	LOW	ISD should monitor the performance targets specified in the SLA.
8.6	LOW	ISD should ensure that performance reports are produced to measure the attainments of objectives stated in the SLA.
Ref: Chapter 5.3 MANAGEMENT OF INFRASTRUCTURE – Change Management and Release Management		
9.1	MEDIUM	Technical Support group should implement more rigorous change management and release management processes to document changes to the infrastructure, and communicate the nature of the changes to users and provide users with information on the impact of the implementation.
Ref: Chapter 6.1		**SYSTEM DEVELOPMENT – Special projects**
10.1	LOW	ISD should describe the term “special project”.
10.2	HIGH	Where the scope warrants, ISD should describe and prioritise special projects in the IT plan.
10.3	LOW	ISD should ensure that a project plan is developed for each project.
10.4	LOW	Where the scope warrants, ISD should ensure that the development process follows a formal SDLC.

APPENDIX B: AUDIT BACKGROUND INFORMATION

B1: Audit Objectives

Two audit objectives were identified for the audit of Information Technology (IT).

1. Assess the ISD management control framework to ensure that the IT function is efficiently and effectively managed.

2. Review and examine all ISD lines of services, IT operational activities, technological functions, and main processes and assess the appropriateness, efficiency and effectiveness of each one.

B2: Audit Scope

The main focus of the audit was the Information Technology Division. The audit covered:

- The management control framework related to ISD as illustrated in Appendix F.
- All operational IT functions, services, processes, and activities provided by ISD as presented in Appendix F.
- The Information Management, Record Management, and Knowledge Management functions were excluded from the audit work.
- The application systems and applications such as ESD, eBusiness, AMIS, NAMIS, and Business Intelligence were also excluded from the audit work. However, the general System Development processes were included.

B3: Methodology

This audit is a common audit that deals with both Councils. The recommendations that are included in this report apply to both Councils. To ensure a wide coverage for data collection, interviews were conducted with more than 40 interviews representatives (see Appendix E) of the

- Natural Sciences and Engineering Research Council of Canada (NSERC),
- Social Sciences and Humanities Research Council of Canada (SSHRC), and
- Common Administrative Services Directorate (CASD).

The methodology used during the audit is Progestic proprietary. As such, it was developed over the years using diverse well-known sources. All the following sources were used to create an integrated audit methodology:

- Control Objectives for Information Technology (COBIT),
- Infrastructure Library for Information Technology (ITIL),
- Treasury Board Secretariat - Government Security Policy audit guide,
- Treasury Board Secretariat - System Under Development audit guide,
- Treasury Board Secretariat - An Enhanced Framework for the Management of Information Technology Projects,
- Treasury Board Secretariat - Operational Security Standard - Business Continuity Planning (BCP) Program, and
- Treasury board Secretariat - Management of Information Technology policy.

Appendix F provides a visual representation of the audit topics included in our methodology.

- The top portion of the diagram highlights the seven (7) management control framework functions that were reviewed, and
- The lower portion of the diagram provides a detailed list of IT operational functions that were examined during our audit.

The audit was conducted in three distinct phases.

1. In August and September 2004, a preliminary survey was completed to confirm the audit objectives and IT managerial and operational functions to be audited in the audit execution phase. Criteria were developed to support the audit objectives and an audit program was produced to identify the information that will be collected during the audit execution phase.

2. In September, October and November 2004, the audit execution phase was completed to collect relevant information (interviews, document reading, and visual observations) on the ISD management control framework and operational functions.

3. In November and December 2004, the Reporting Phase concentrated on finalizing the analysis of information, completing the audit program with the information collected through interviews and document reading, producing a Power Point presentation for the Director ISD, drafting the draft version of the audit report, and structuring the working paper files.

B4: Acknowledgements

Progestic would like to thank all NSERC, SSHRC and CASD managers and staff who participated in this audit. Their co-operation and assistance in helping us carrying out our assignment was instrumental in identifying and assessing the service level provided by ISD.

APPENDIX C: ISD - BACKGROUND INFORMATION

Background – To provide administrative services to the NSERC and SSHRC Councils, the CASD organization was created. It regroups several administrative entities such as Finance, Human Resources, Administration and Information Services Division (ISD).

Information Services Division (ISD) - Over the years, ISD invested time, effort and resources in the development, implementation and maintenance, including the upgrading of its IT. ISD services include the support and delivery of an Office Automation environment provided to staff members of Both Councils. The mission of ISD is to help meet the NSERC and SSHRC's program objectives by leading and supporting the effective use of IT. ISD provides guidance, service and support on informatics to NSERC, SSHRC and CASD staff located in Headquarter or regional offices. ISD is responsible for:

- The IT planning and direction of both Councils;
- The efficient operations of the IT infrastructure as well as the necessary support to cover the business needs of both Councils and adequate dissemination of information;
- The preparation and circulation of IT documentation covering equipment usage, system security and procedural implementation relative to computers and systems;
- The provision of Data Administration services including data management, technical communications, Intranet and data architecture;
- The management and operations of Helpdesk support groups for internal and external clients; and
- The System development and maintenance of core applications and special projects. Several corporate information systems support the delivery of core programs, notably the NSERC NAMIS and eBusiness systems, the SSHRC AMIS and ESD online application, and the CASD FPAM, SMS and HRIS systems.

Within ISD, there are six responsibility centres (RCs). The Director, ISD has one and each one of the five ISD Managers has its own RC and is responsible to manage and control its own budget (salary and O/M).

As of December 1, 2004, ISD had a total of 77 people composed of 56 staff and 21 consultants. The distribution of staff between the two councils is:

1. 19 (34%) staff dedicated to SSHRC, and
2. 37 (66%) staff dedicated to NSERC.

Table 1 illustrates the distribution of staff and consultants across ISD for each responsibility centre.

Table 4: BREAKDOWN OF ISD STAFF AND CONSULTANTS IN ISD			
ISD GROUPS	**TOTAL**	**MANAGERS AND STAFF**	**CONSULTANTS**
TS - Special projects	4	3	1
TS - Database administrators	3	3	0
TS - Technical Support	4	4	0
TS – Security	1	1	0
Total TS (Technical Services) group	**12**	**11**	**1**
DA - Data Administration SSHRC	3	3	0
DA - Data Administration NSERC	3	3	0
DA - Intranet Group	3	1	2
DA - Technical writing	3	2	1
Total DA (Data Administration) group	**12**	**9**	**3**
HD – ISD Helpdesk	4	4	0
HD - Information Technology Analysts	4	4	0
Total HD (Helpdesk) group	**8**	**8**	**0**
SD1 - System Development and maintenance for NAMIS	7	3	4
SD1 - System Development and maintenance for AMIS	7	5	2
SD1 - System development – Business Intelligence	4	3	1
SD1 - System development and maintenance for ESD	4	2	2
Total SD1 (System Development) first group	**22**	**13**	**9**
SD2 - eBusiness and ESD Helpdesk services	5	2	3
SD2 - System Development for NSERC eBusiness	11	6	5
Total SD2 (System Development) second group	**16**	**8**	**8**
TOTAL number of staff less first line managers	**70**	**49**	**21**
TOTAL ISD: Director (1) + First line managers (5) + Administrative assistant (1)	**7**	**7**	**0**
TOTAL	**77**	**56**	**21**
% of workforce category		**56/77 = 73%**	**21/77 = 27%**

Number of staff involved in the system development and maintenance functions – The number of staff involved in system development and maintenance functions was estimated by identifying staff involved in the delivery of functional activities included in the system development life cycle: user requirements, functional specifications, programming, quality assurance, data base administration and data administration, change / release management.

Furthermore, we considered that ISD was involved in two distinct types of system development and maintenance activities:

1. Business applications (eBusiness, NAMIS, AMIS, ESD, FPAM, SMS, HRIS), and
2. Other applications often referred to as Special Projects (Portal project, Intranet, Business Object reports, FDSR, Common CV, Common Grant System, Family Album, IMEP, ECIMS, eScoring, and many more.

We estimated that 24 staff are involved (either full time or part-time) in the development and maintenance of special projects. This represents 31% of ISD workforce (24/77) and 43% of the total ISD system development workforce (24/56). It is however important to note that these staff have other duties and the activities related to system development and maintenance are only one of their responsibilities. More details are provided on this issue in Chapter 5.3 (system development and maintenance).

Table 5: IDENTIFICATION OF STAFF INVOLVED IN THE SYSTEM DEVELOPMENT AND MAINTENANCE ACTIVITIES

ISD GROUPS	TOTAL	MANAGERS AND STAFF	CONSULTANTS
STAFF INVOLVED IN THE DEVELOPMENT OF SPECIAL PROJECTS			
TS - Special projects	4	3	1
DA - Intranet Group	3	1	2
HD - Information Technology Analysts	4	4	0
SD1 - System development – Business Intelligence	4	3	1
TOTAL SPECIAL PROJECTS	**15**	**11**	**4**
STAFF INVOLVED IN THE SYSTEM DEVELOPMENT OF CORE APPLICATIONS			
TS - Database administrators	3	3	0
DA - Data Administration SSHRC	3	3	0
DA - Data Administration NSERC	3	3	0
SD1 - System Development and maintenance for NAMIS	7	3	4
SD1 - System Development and maintenance for AMIS	7	5	2
SD1 - System development and maintenance for ESD	4	2	2
SD2 - System Development for NSERC eBusiness	11	6	5
ISD first line managers	3	3	0
TOTAL ISD staff identified in system development	**41**	**28**	**13**
TOTAL # OF PEOPLE INVOLVED IN SYSTEM DEVELOPMENT ACTIVITIES	**56**	**39**	**17**
TOTAL ISD STAFF (EMPLOYEES AND CONSULTANTS	**77**	**56**	**21**

Salary breakdown - Salary breakdown within the SMS financial system has allocated 36.4 staff (representing 66% of total ISD staff) to NSERC while 19.6 staff (representing 34%) of total ISD staff) are allocated and paid by SSHRC.

ISD budget for fiscal year 2004 – 2005 - The discussions with the Director ISD has shown that for fiscal year 2004 – 2005, ISD budget remained essentially the same as the one approved for the 2003-2004 fiscal year. A slight decrease of $200,000 and $100,000 was experienced for NSERC and SSHRC respectively. The ISD combined budget still exceeds $8.5 millions, out of which $3.6 millions represent salary and overtime costs.

APPENDIX D: INCREASING COMPLEXITY OF IT

The IT function is becoming more and more complex. Today, organizations have become dependent on the availability, security, and reliability of IT services. Without IT, it is difficult, if possible, for users to achieve their business objectives. Program and Service staff rely on the availability of corporate applications, networked infrastructure, Internet, e-mail and office automation tools to conduct their day-to-day business. Far are the days where computer specialists were managing a mainframe computer environment providing central processing power and linking green screen dumb terminals through dedicated telecommunication lines. IT evolved from a centralized mainframe environment to become a decentralized and distributed environment. Microcomputers (PCs) replaced dumb terminals; Local Area Networks (LANs) were introduced to link most PCs; then Wide Area Networks were introduced to link all LANs, and for many years, minicomputers and client servers have since replaced mainframe computers.

Today's technological infrastructure contains more components and is more vulnerable than before. Not only is the environment becoming more complex, but also the boundaries are expanding outside the scope of the Councils. Most federal departments, including NSERC and SSHRC want to link with other government Departments, and reach Canadian people and Canadian organizations using Internet. These new "e-Business" ways of doing business also forced organizations, including ISD, to step outside of the relative safety of its own IT Infrastructure. Now risks need to be tightly managed to protect the network and the corporate data against threats originating from the outside world.

Additional pressures are currently exercised on ISD to provide a flawless infrastructure that will provide tomorrow's services. During this lengthy and fragile transition period, ISD must remain focussed on enhancing and maintaining its current IT environment and protect it against threats and risks that prevail. Hence, ISD services and infrastructure need to be of high quality and stable so that service levels and network availability may continue to support daily operations.

The IT world is a very dynamic world. It changes constantly and new technologies are introduced at a rapid pace. Contrary to Finance, Human Resources, and Procurement, IT staff are constantly facing an expanding technological world. Every month, Hardware and Software Suppliers introduce new technical possibilities to interconnect technologies, many of which revolutionize the way people do business or use technology. For example, the Internet expanded the horizon of system development and gave birth to eCommerce; the Personal Digital Assistants (PDA or palm held device) introduced new ways to connect to the network, send e-mails, receive mail, and connect to the Internet; VoIP (Voice over Internet Protocol) allowed users to make telephone calls using a computer network, over a data network like the Internet and gave birth to Teleconferencing; and so many more.

Most of the time, users are aware of these new technologies and put pressure on the IT organization to adopt them in order to enhance the current office automation capacity or improve their business processes. However, they are unaware of risks, costs, or impact on the current infrastructure of adopting them.

Increasing security measures - Along with the advance of technology, new threats were introduced in the IT world. Every month, new risks are surfacing many of which have their own unique name and terminology: For example with the spreading of Internet uses, the IT world has experience several new threats such as VIRUS, SPAM, identity theft, data corruption, breaches in confidentiality, spyware on the network, hackers, etc.

Success with IT - Over the years, ISD has been successful. Through the downsizing period, ISD was successful in keeping its IT spending to a minimum, while offering many new services, and improving the functionality of the NAMIS and AMIS business applications. The careful evolution of the telecommunication backbone and constant upgrades in hardware and software standards were instrumental in the implementation of the e-mail Outlook system and the Microsoft Suite office automation suite of software products. The centralisation of LANs and production servers in ISD provided a more stable operational environment. Other successes are the implementation of the shared systems for finance (FPAM and SMS) and human resources (HRIS), the adaptation to constantly evolving technology, and keep up with the rapid growth in Office automation services. All these challenges were met while offering a relatively stable support to users for their corporate applications, and office automation hardware and software.

Increasing pressures on ISD – In the early 2000, NSERC and SSHRC decided to review their business processes and endorsed the Internet route to do business with their clients. And to make things even more complicated, several organizations including NSERC and SSHRC no longer think of System Integration but are planning for Business Integration. In this context, both Councils are currently redesigning their business processes and developing the NSERC eBusiness projects and enhancing the SSHRC ESD on-line application systems.

While this is happening, some older business applications need to be maintained and others need to be re-written and converted to newer technologies because software vendors no longer support the software language (Power Builder) that was initially used to develop these applications. This is the case of the NSERC NAMIS and SSHRC AMIS applications.

The need for continual integration with every new application put a massive maintenance overhead on the IT department's operation. Within ISD, System development and maintenance staff and consultants represent 79% of ISD workforce or 61/77 staff and consultants represent 26% of ISD workforce (20/77) or 95% of all ISD consultants (20/21).

These pressures on ISD are caused by growth in business and technology needs, the need to target a better value-for-money due to budget constraints, diversity and rapid change of technology, changing business requirements, increased users' expectations, and increased complexity of user support. One of the main issues confronting ISD management today is trying to provide cost-effective support and IT services to a more demanding audience due to the increased reliance on computers technology.

This environment provides solid evidence of the escalating complexity of IT, and justifies the growing need to hire qualified IT personnel and keep the staff constantly trained and educated on current technologies. To complement basic education, many Software Vendors developed their own accreditation programs so that IT staff understand and maintain their hardware (such as Microsoft Software Engineer (MSE), Microsoft Software Certified Engineer (MSCE)), software

(Oracle (OCP)), and provide quality IT services such as Helpdesk (HDI). Some ISD staff acquired some of these accreditations.

Managing an IT organisation in 2004 is quite a challenge. Not only does ISD staff have to maintain current technologies, computer applications, and network operations, they have also to secure the environment, keep informed on new technology trends and enhance the current IT environment. All this has to be done within the financial constraints the federal government imposes on departments, and the department imposes on its IT organization. Furthermore, as ISD is trying hard to maintain its current environment, program people are constantly modifying their business programs, reviewing their business processes, and finding new ways to reach their clients by using new technology.

APPENDIX E: LIST OF PEOPLE INTERVIEWED

#	FAMILY NAME	FIRST NAME	TITLE	ORGANIZATIONS		
				CASD	NSERC	SSHRC
1.	Alper	Anne	Manager - RPP Planning and Budget Team		X	
2.	Baker	David	Consultant – CGS and CCV	X		
3.	Beaureguard	Léo	Senior Information Technology Analyst – ISD	X		
4.	Bellemarre	Guy	Senior Analyst, Development Team Leader	X		
5.	Blain	Isabelle	Vice President - Research Grants and Scholarships Directorate		X	
6.	Blain (2)	Daniel	Support Centre Manager – ISD	X		
7.	Bouchard	Gérald	Quality Assurance Analyst – ISD	X		
8.	Boucher	Christian	Project Officer - Regional Offices Division			
9.	Brown	Steve	Help Desk Analyst – ISD	X		
10.	Budarick	Vannessa	Senior Analyst, Development Team Leader – ISD	X		
11.	Cavallin	Michel	Director General - Common Administrative Services Directorate	X		
12.	Chateauvert	Tom	Project Manager – ISD	X		
13.	Dunne	Patricia	Director, Fellowships and Institutional Grants			X
14.	Fonda	Marc	Program Officer - Strategic Programs & Joint Initiatives			X
15.	Godin	André	Web Developer / Analyst. – ISD		X	
16.	Gravel	Marc	Chief Web Development		X	
17.	Heyerdahl	Martha	Coordinator, Security and Projects – Administration Division	X		
18.	Halliwell	Janet	Executive Vice President - Executive Vice-President's Directorate			X
19.	Hull	André	Information Technology Analyst	X		
20.	Lamarca	Mario	Director - Engineering and Program Operations Unit		X	
21.	Laplante	Diane	Senior Data Administrator		X	
22.	Leblanc	Michel	Manager, Planning, Reporting and Systems	X		
23.	Leduc	Patricia	Quality Assurance Team Leader – ISD	X		
24.	Lee	Debbie	Project Manager - ISD	X		
25.	Leonard	Paul Eric	Team Leader – eBusiness Helpdesk - ISD		X	
26.	Levesque	Pierre	Senior Officer - Knowledge Products & Mobilization			X
27.	Lloyd	Nigel	Executive Vice President - Executive Vice-President's Office		X	
28.	Meilleur	Nathalie	Senior Internal Auditor - Policy and International Relations Division		X	
29.	Mercer (3)	Kalvin	Director ISD	X		
30.	Michault	Nicole	Manager Electronic Services Delivery			X
31.	Moore (2)	Cliff	Technical Services Manager – ISD	X		
32.	Nolan	Cynthia	Technical Communications Analyst – ISD	X		
33.	Popescu	Silviu	Application Design Analyst – ISD	X		
34.	Potvin	Norman	Web Developer – Communication Division		X	
35.	Quirouette	René	Director Administration	X		
36.	Rainville	Marie Ginette	Project Coordinator - eBusiness Project		X	

#	FAMILY NAME	FIRST NAME	TITLE	ORGANIZATIONS		
				CASD	NSERC	SSHRC
37.	Régnier	Hélène	Senior Policy Analyst - Corporate Policy and Planning			X
38.	Robillard	Josie	Senior Data Administrator			X
39.	Séguin	Mylène	Program Assistant - Fellowships & Institutional Grants			X
40.	Shields	David	Chief Information Management	X		
41.	Shugar	Steve	Director - Policy and International Relations Division		X	
42.	Squires	Shirley	Director Human Resources	X		
43.	St-Jean (4)	Denis	Network Architect – ISD	X		
44.	Villemure	Christiane	Director - eBusiness Project		X	

APPENDIX F – VISUAL REPRESENTATION OF AREAS THAT WERE ADDRESSED DURING THE NSERC - SSHRC "IT" AUDIT

AUDIT OF INFORMATION TECHNOLOGY

MANAGEMENT CONTROL FRAMEWORK

ORGANIZING	LEADERSHIP	PLANNING	ADMINISTERING	RISK MANAGEMENT	CONTROLLING	COMMUNICATING
• Structure (reporting, roles/responsibilities, accountability, authority, relationship, committees) • Mission, mandate, objective, scope • Effectiveness of structure • Staffing (number, classification, qualification) • Use of contracting	• Policies • Procedures • Standards • Guidelines • Methodologies • Client satisfaction	• Operational plan • Long term IT plan • Strategic IT plan • Budget • Implementation strategy • Priority setting • Performance measurement	• BRP • DRP • TRAs • SOS • PIAs • Inventory	• Workload • Skill set of staff • Training • Working environment	• Progress reporting • Monitoring practices • Budget control • Project control	• Awareness strategy • Internet and Intranet content • Committees (internal / external) • Communication with users

INFORMATION TECHNOLOGY OPERATIONAL ACTIVITIES

ADMINISTRATIVE PROCESSES	SYSTEM DEVELOPMENT / PROJECT MANAGEMENT	NETWORK MANAGEMENT & TELECOMMUNICATION	HELPDESK	COMPUTER OPERATIONS	SECURITY	INTERNET INTRANET EXTRANET	
• Budget • Contracting • Purchasing (micros, servers, disposal, inventory, software, license control,) • PCs at home	**OPERATIONAL MCF** • SDLC Methodology • PM methodology • Users involvement • Ownership of applications • Change management • Release management • Implementation strategy • Progress control • Committee structure • Project control • Documentation • Post implementation review • TRAs • Workload • Use of contractors • Training	**OPERATIONAL MCF** • Authorisation / authentication (establishment of user profile (need to know), logon id, password management, frequency of change, • Firewalls • Virus protection • E-mail protection • Work at home / telework / remote access • Backup practices (frequency, types, off site storage, • IP addresses • Privileged access • Log monitoring • Video conferencing • Contractors	**OPERATIONAL MCF** • SLA • Performance indicators • Escalation procedures • Staffing (skill sets, levels, experience) • Recording of calls • Systems used • Reporting • Service mentality • Communications • Trend studies • Workload • Support of PC at home • Types of services provided • Training • Effectiveness • Reputation	**OPERATIONAL MCF** • Policies, procedures, standards • Control • Quality of service • On-line systems control • Software and telecom support • Mgt support functions such as problem mgt, change mgt, security, utilisation reporting and control, training of computer centre staff • User satisfaction (up time, availability, responsiveness, communication of changes	**OPERATIONAL MCF** • Access rights • User profiles • Personnel • Physical • Logical • Hardware • Software • Network • Telecom • Internet • Intranet • Extranet • Operations • Etc.	**OPERATIONAL MCF** • Policies, procedures, standards • Firewalls • Development • Centralisation vs. decentralisation • Contractors • Management of content • Authorisation, authentication • Virus protection • PKI • E-commerce & E-Business • Management of IP addresses • Bandwidth • Remote access	