Executive Summary

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 realizes the expected benefits,
- IT exploits opportunities and maximizes 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.

    o 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.

    o 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, prioritize, 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.

    o 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.

    o 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 capitalize 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.