AUDIT OF THE

MANAGEMENT OF THE INTRANET

January 2006

Foreign Affairs Canada
Office of the Inspector General
Audit Division (ZIV)

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Conclusion

This audit was approved by the Departmental Audit and Evaluation Committee for 2004 - 2005 and was conducted during the period from November 1, 2004 to March 22, 2005. The Intranet was identified as a key management concern by the Chief Information Officer during annual management consultations, undertaken when planning departmental audits.

Overall, we believe this report will help management better understand and enhance its use of the Intranet as a corporate communications tool. The report also provides clear recommendations against which future spending on the Intranet can be assessed. The overall conclusion of the audit is that FAC is not realizing potential returns on its investment in the Intranet.

The audit found that the overall management framework for the governance of the FAC Intranet lacks a clear strategic direction. Inaccurate and outdated content on some FAC Intranet Web sites has reduced user confidence in all Intranet content. There is a need to improve processes and quality controls for managing, maintaining and withdrawing content published on the FAC Intranet.

The audit revealed limited user awareness of the content available on the FAC Intranet. Many FAC Intranet Web sites are unstructured and difficult to navigate, search engines are ineffective and frustrating, and the effective capacity of the network at some missions is not sufficient to access this information. Some missions (Paris, London, Washington, etc.) had Intranet sites that were not compliant with the Official Languages Policy. The audit also raised issues related to security, Intranet technology and application consolidation, and tracking the costs of ownership.

The audit recommends establishing a governance structure, developing an Intranet strategy, implementing content standards and related quality controls, improving search functionality, ensuring missions have adequate effective capacity for their Intranet needs, and mitigating security risks related to Intranet content. The audit recommends that the DMA assign responsibility for the management of the Intranet to the Communications Bureau (BCD). To implement the recommendations, it is recommended that an Intranet Steering Committee and an Intranet Editorial Board be established. This report assumes that there will be ongoing participation from the office of the Chief Information Officer (CIO) in all aspects of the emerging governance structure for the Intranet.

During audit briefings, we noted that the department has already taken concrete steps to establish a framework in which to implement key components of the report. As with any undertaking of this magnitude, the implementation of the recommendations should be phased and in consideration of the operational constraints of content owners.

Objectives

The objectives of the audit were to:
- assess the overall management framework for the governance of the Intranet;
- assess the efficiency and effectiveness of the Intranet implementation in meeting user requirements;
- assess whether standards and policies for availability and integrity are being met; and

- identify and promote best practices noted during the audit.

Audit Criteria

The audit was performed in accordance with Treasury Board Policy on Internal Audit and the requirements and guidelines outlined in "The Professional Practices Framework" of the Institute of Internal Auditors (IIA).

The audit criteria were based on applicable COBIT[1] requirements, as well as departmental and Treasury Board Secretariat policies and procedures. Sufficient audit work has been performed and the necessary evidence gathered to support the conclusions reached in this audit report.

MAIN POINTS

Audit findings are presented in the following categories:

1. Governance and Overall Management Framework
2. Efficiency and Effectiveness of Intranet
3. Meeting Standards for Availability and Integrity

- The audit also included best practices, with the emphasis on identifying existing strengths noted during the audit which could be shared with stakeholders in both departments. In addition, Best Practices available from COBIT[2] and ITIL[3] are presented in Appendix C.

Governance and Management Framework

Roles and Responsibilities

- There is no executive level steering committee with the explicit mandate to establish strategy, develop policies, and ensure that they are implemented. Consequently, individuals operate independently and make more narrowly-based decisions, resulting in an overall lower level of operational effectiveness.

- There is no strategy that links the overall departmental goals to the goals and objectives for the intranet, and to policies for management of information content and of the intranet infrastructure. This lack of direction is the root cause of many of the other problems observed during this audit. Furthermore, it inhibits the ability of the existing management structure to address and resolve these problems.

- The lack of clarity regarding the fundamental purpose and role of the FAC Intranet causes conflicting understanding and interpretation by management and staff. This, in turn, creates inefficiencies through duplication, conflicts, and unmet user needs.

---

[1] Control Objectives for Information and Related Technology: Information Systems Audit and Control Association, see details Appendix C.

[2] **Control Objectives for Information and Related Technology**: Referenced by Treasury Board Secretariat for the conduct of assurance engagements related to Information Technology.

[3] **IT Infrastructure Library**: ITIL has become the worldwide de facto standard in Service Management.

- In order to make traction on the key findings of this audit, the department needs to assign responsibility for the management of Intranet content to the Communications Bureau (BCD). To implement the recommendations, an executive level Intranet Steering Committee and an operations level Intranet Editorial Board need to be established. This report assumes that there will be ongoing participation from the office of the Chief Information Officer (CIO) in all aspects of the emerging governance structure for the Intranet.

Management of Content

- The content of the FAC Intranet is not regulated by consistent operational-level management direction and controls. There is considerable variation across Intranet sites and development environments. This leads to inefficiencies and frustrations for the users, and higher support costs.

Cost of Ownership

- Although there is some anecdotal evidence of cost tracking, in general the department does not know the costs of the Intranet related to managing, publishing, maintaining, and retiring Intranet content. Consequently, governance of the intranet must be performed without a key piece of information to support management decisions. The audit identified areas for increased efficiencies and potential cost reduction by harmonizing application development technologies and environments.

Efficiency and Effectiveness of the Intranet

User Dissatisfaction

- FAC Intranet Web sites fail to meet user needs, contain unreliable content, lack feedback channels and have different appearances and unfamiliar Web site layouts. Overall, FAC Intranet content is very inconsistent and inefficient to access. This has resulted in many user complaints and frustration.

Structure and Usability of the Panorama Web Site

- The current form of the primary FAC home page – the Panorama Web site – is widely considered to be unstructured, difficult to navigate, unfriendly to users, and largely a duplication of content with broadcast emails. This makes it inefficient and ineffective as a tool for accessing FAC information.

Effectiveness of Search Engine

- The configuration of Search Engines on the Intranet is ineffective and involves several separate, non-integrated engines that are implemented in an inconsistent manner. The result to the user is slow operation, incorrect results, and overall frustration. This, in turn, leads users to seek their information through less efficient means, such as manual searches, paper searches, or personal contact.

Intranet Application Development Technologies and Environments

- There may be opportunities to reduce Intranet application development costs through harmonizing application development technologies and environments.

Availability of Intranet to Missions

- Users at some missions are unable to utilize Intranet applications and work tools which are intended to improve productivity. This is due to limited effective capacity. Effective capacity is a function of the network link speed, the applications being used, user patterns and the proper tuning of applications and network. The audit includes recommendations to resolve these capacity constraints and improve mission usage without incurring additional costs for bandwidth upgrades.

Intranet Security

- The lack of quality controls on material being published to the Intranet has management concerned that there may be sensitive information on the Intranet that may individually or collectively compromise security.

Meeting Standards for Availability and Integrity

- The integrity of the content of some of the reviewed Web sites is low, which exacerbates the efficiency and effectiveness problems noted elsewhere in this report. Inaccurate and outdated content on some FAC Intranet Web sites has contributed to widespread scepticism by staff regarding the accuracy of all Intranet content. User access to Intranet content has been negatively impacted by a lack of commonly accepted page layouts and navigation, and search engines that simply do not work.

AUDIT APPROACH

Audits are performed to provide management with assurance that control objectives are being met, to identify where there are significant control weaknesses, to substantiate the resulting risks, and to advise management on necessary corrective actions.

Background

The Foreign Affairs Canada (FAC) and International Trade Canada (ITCan) Intranet is a corporate tool for the electronic dissemination of departmental communications, tools and services to all employees at Headquarters and the missions. The Intranet was established in order to provide a cost-effective, user-friendly means of internal communications. Initially, the Intranet Web site was developed by the Information Management Technology Bureau. The Intranet is used to disseminate documents such as departmental manuals and directives, Division Web sites, and Panorama broadcast messages. The Intranet also provides access to tools such as the on-line Department directory, and services through applications such as the Human Resources Management System (PeopleSoft). The Intranet uses Internet (World Wide Web) type tools, but is set up on the internal SIGNET network.

The contents of the intranet are not "owned" by the Information Management Technology Bureau, nor is the establishment of an intranet site under any form of centralized "approving" organization within the departments. During annual management consultations the Chief Information Officer identified the Intranet as a key management concern, in particular that there were issues of governance, accuracy or "currency" of content, and ongoing costs that needed to be addressed. In addition, the separation of FAC and ITCan into two departments underscored the need to undertake a comprehensive audit of the Intranet.

1.1 Scope

The scope of the audit included both the FAC and ITCan Intranets. The audit addressed the areas of:

- Governance and overall management framework;
- Satisfaction of user and business requirements;
- Ongoing costs of ownership;
- Accuracy and currency of content; and,
- Availability and integrity of systems.

1.2 Methodology

The audit deliverables and key audit activities included:

- **Project Plan**: a detailed project plan identifying deliverables, milestones and resource usage.
- **Auditee Selection and Interview Coordination**: interviews were arranged and conducted with thirty-two auditees.
- **Audit Program Design**: an audit guide linking audit criteria with audit objectives was developed and applied.
- **Interview Question Design**: interview questions based on the audit objectives and criteria were prepared and applied.
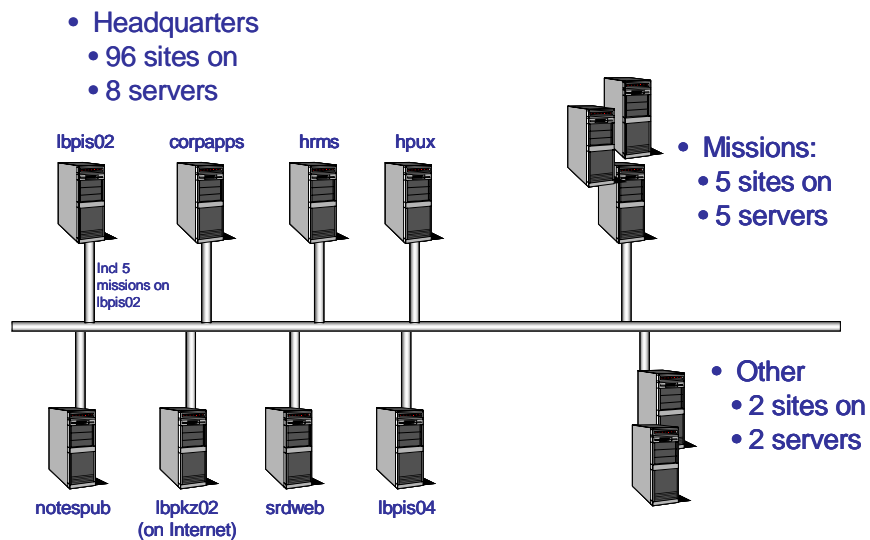
- **Auditee Interviews**: audit interviews were performed and documented.
- **Technical Analysis**: an automated Web site analysis tool was used to derive specific Intranet technical and performance metrics.
- **Management Briefings**: audit findings and recommendations were presented and briefing notes maintained.
- **Audit Report**: a draft report was prepared that identifies areas of concern with clear linkages between observations, cause and effect and recommendations.
- **Working Papers**: working papers, interview notes and analysis documents were prepared and maintained electronically.

1.3 Sampling Technique and Technical Analysis

A structured sampling approach was used to ensure that the sample represented a broad cross section of Intranet stakeholders, content owners, users and technicians. Although the audit did not survey a large number of managers or employees, interviews were supplemented with the use of electronic tools which allowed testing of Web sites not possible using a manual approach.

"Watchfire", an automated Web site analysis tool, was used to derive specific Intranet technical and performance metrics, including dead links and the efficiency of search engines. The detailed Watchfire reports were run on the primary Intranet server and the results are presented in Section 3.0 of this report.

The ninety-six (96) Web sites examined during the audit resided on the following eight (8) servers at headquarters and are depicted on the high level network diagram below:

- Headquarters
  - 96 sites on
  - 8 servers

lbpis02   corpapps   hrms   hpux

- Missions:
  - 5 sites on
  - 5 servers

Incl 5 missions on lbpis02

- Other
  - 2 sites on
  - 2 servers

notespub   lbpkz02 (on Internet)   srdweb   lbpis04

Intranet Servers Audited

1.4 Interviews

Detailed interviews were conducted with a sample of Intranet stakeholders, users, Intranet content owners, webmasters, division and departmental management. Some interviewees had several roles related to the Intranet (e.g., webmaster and Intranet user) and received multiple audit questionnaires during the interview.

A list of interviewees is provided in Appendix A.

The primary server, lbpis02, contained most of the Intranet Web sites audited, including the Panorama homepage which (at the time of the audit) was Foreign Affairs Canada's primary Intranet Web site. Many Intranet Web sites are accessed through links on the Panorama homepage, including Web sites residing on other network servers. The primary Intranet server (lbpis02) is also host to five (5) mission sites (i.e., Beirut, Brussels, Belgrade, Manilla, Oslo). The audit also reviewed five (5) other missions on other servers (i.e., Tokyo, New Delhi, Washington, London, Paris), and two other sites on two other servers on the Intranet.

The number of sites audited on each server is listed in the table below.

Server	URL	Primary Role	Total Sites
lbpis02	http://intranet	Panorama PLUS others	70
lbpk01	http://corpapps	EQAMS, PubReg, Directory	3
160.106.180.189	http://hrms-sgrh.dfait-maeci.gc.ca	PeopleSoft	1
lbpcat01	http://lbpcat01.capps	CATS, Tech Library	1
lbpk06	http://notespub01.dfait-maeci.gc.ca	Competitions, Acq Pol DB	2
albertpr	http://srdweb	Property, Materiel, Mail	1
lbpkz02 (on Internet)	http://pubx.dfait-maeci.gc.ca	Pubs Catalog	1
lbpis04	http://intranetapps	Various Applications	17
TOTAL			96

1.5 Planning and Monitoring

A detailed audit plan identified all audit activities and the audit schedule. The status of the audit was monitored through weekly team meetings and through bi-weekly status reports. These meetings also provided an opportunity for the audit team to leverage ZIV organizational knowledge and guidance.

DETAILED FINDINGS

1.0 Governance and Management Framework

1.1 Governance of the Intranet

There is no executive level steering committee with the explicit mandate to establish Intranet strategy, develop related policies, and to ensure that they are implemented. Consequently, individuals operate independently and make more narrowly-based decisions, limiting Intranet effectiveness.

There is no strategy which would link the overall departmental goals to the goals and objectives for the Intranet, to the policies for management of information content, and to the Intranet infrastructure. This lack of direction is the root cause of many of the other problems observed during this audit and inhibits the resolution of these problems.

The lack of clarity regarding the fundamental purpose and role of the FAC Intranet causes conflicting understanding and interpretation by management and staff. This, in turn, creates inefficiencies through duplication, conflicts, and unmet user needs.

Many Intranet content owners identified the need for an Intranet Steering Committee that would establish the vision and strategy for the Intranet. It was suggested that the vision state the purpose of the Intranet and how Intranet content can assist in achieving corporate objectives.

An unclear understanding of the role and purpose of the FAC Intranet has contributed to difficulties in establishing priorities, inefficient decision making, and significant variations in the quality of FAC Intranet content. Although Intranet <u>infrastructure</u> operates efficiently, the <u>content</u> (material) on the FAC Intranet is not being effectively used to support internal communications.

Without a defined role and purpose for the Intranet, decisions may be based on unclear priorities and effort may be expended on initiatives that do not relate to making the FAC Intranet a more efficient and effective corporate communication tool. However, defining the role and purpose of the Intranet will not yield benefits unless it is clearly communicated to managers and staff with Intranet responsibilities.

There is a need for a high level strategy for the Intranet that clearly defines the role and purpose of the Intranet as a corporate communications tool. Communication paths may be between individuals, between departments, between departments and individuals, and between managers and staff, etc. The strategy and governance structure for the Intranet should address:

- the corporate vision and role of the Intranet as a communications tool;
- the roles and responsibilities associated with the Intranet and its content, including responsibilities related to Intranet infrastructure;
- the policies and procedures related to the publishing, maintenance and removal of Intranet content;
- Intranet design standards and guidelines to achieve communication objectives;
- the priorities and balance of technical and user/communications priorities; and,
- the quality control and quality assurance practices (e.g., review points, approval authorities, etc.).

The Communications Division (BCD) currently manages the Department's Internet Web site. Like the Department's Internet site, the Intranet should be managed by communications experts within FAC. This report assumes that there will be ongoing participation from the office of the Chief Information Officer (CIO) in all aspects of the emerging governance structure for the Intranet.

The Horizons Intranet Web site was observed to have a clearly communicated role and purpose. Its mandate is to support ITCan personnel in the field with "usable and actionable" content. Its policies and standards are defined by a committee of stakeholders, and quality controls are implemented by the Horizons Team. The audit found that Horizons content was current, consistent with user need, and widely used by Trade Commission Service employees.

Recommended that:

1.1.1   DMA assign responsibility for the management of the Intranet to BCD. This recognizes the Intranet as a corporate communications tool.

1.1.2   BCD set-up an Intranet Steering Committee that is executive level and broadly based. The Steering Committee should clearly define:
- **the role and purpose of the Intranet as a corporate communications tool;**
- **the policy for operational governance;**
- **the policy for content management; and,**
- **the policy for design standards.**

Action and Time Frame

1.1.1   DMA agrees. BCD was assigned the responsibility for managing the Intranet at the Management Committee meeting of April 20, 2005. Management committee also agreed to the following items:

- **The need for an Intranet strategy -- and a governance structure;**
- **The need for an Executive Level Intranet Steering Committee;**
- **BCD to take the role of leader, not operator.**
- **The need for a clean-up exercise, to start soon. This exercise must take into account communicating with users, content owners, and technology providers. The audit identified a number of orphan sites. Prior to deleting these and other material, proper analyses must be conducted, driven through an Editorial Board.**

   Time Frame: Management Committee has now charged SCMA with the task to estimate the overall resource requirements for an Intranet overhaul.

   BCD Response: BCD has accepted responsibility for management of the Intranet and management of the FAC content.

   BCD Time Frame: Dependent on adequate resources.

1.1.2   A co-chaired ITCan-FAC Steering Committee has been initiated and Terms of Reference have been drafted. Additional membership requirements will be determined with the CIO upon approval of Terms of Reference.

Time Frame: Terms of Reference (TOR) completed on Dec 15, 2005.

1.2 Management of Intranet Content

The content of the FAC Intranet is not regulated by consistent operational-level management direction and controls, which allows considerable variation across Intranet sites and development environments. Web site variation leads to user inefficiencies and dissatisfaction, while the variety of development environments contributes to economic inefficiencies.

The extent of quality control is limited and the adherence to existing Web site design guidelines is inconsistent, resulting in significant variation across Intranet Web sites.
The lack of clarity regarding the standards for FAC Intranet Web site layout and appearance leads to user inefficiencies, typically in the form of time lost due to different navigation styles and site layouts, and inconsistent page design conventions. Many users suggested the need for a common structure and appearance to FAC Intranet Web sites in order to reduce the learning curve and improve usability. The efficiency of users is diminished when they are required to learn new Web site layouts. Similarly, development costs are increased as time is spent designing new Intranet layouts.

Existing style guidelines are not followed because they are not considered by webmasters to be adequate or compliant with common Internet conventions. FAC Divisional Intranet Web sites, however, could reasonably be expected to follow standards for "look and feel". Illustrations of some Intranet Web site variation include:

Similarly, this variation of appearances exists among mission Intranet Web sites, including those residing on the main Intranet server:

The criteria and management controls for publication of content to the FAC Intranet are inadequate. The responsibilities for establishing management controls and monitoring compliance are not effectively defined and implemented. Without clear criteria and management controls governing publication of content to the Intranet, ensuring the consistent application of departmental protocols is difficult.

The Department would benefit from the establishment of an Intranet Editorial Board. Its mandate would be:

- to set policies for management of content of Intranet sites;
- to establish operational rules for Intranet content; and,
- to ensure compliance to established rules.

This board would be comprised of webmasters and content owners, or their representatives, from Divisions with significant content on the FAC Intranet. The development and implementation of policies and standards by the Intranet Editorial Board will need to acknowledge the time and budget constraints of Intranet content owners. A phased implementation approach is appropriate.

Recommended that:

1.2.1   BCD establish an Intranet Editorial Board.

      Action and Time Frame

1.2.1   **The framework for an Intranet Editorial Board is being drafted for submission to the Steering Committee when the TOR have been accepted by BCD, CSM, and the CIO.**

Time Frame: Under way, pending approval of the TOR.

1.3 Cost of Ownership

The cost of ownership related to managing, publishing, maintaining, and retiring Intranet Web site content is not being tracked. Consequently, governance of the Intranet does not have the benefit of a key piece of information (i.e., content management costs) that would support good management decisions.

There was interest by senior management in knowing the costs of ownership related to the Intranet so that resources could be better justified or optimized. However, audit interviews clearly indicated that there were no defined processes for determining and tracking the total cost of ownership for the Intranet. The lack of cost data precludes the opportunity to calculate return on investment or undertake comparative benchmarking against other organizations over the longer term.

The only information related to cost of Intranet ownership that was available during the audit were anecdotal estimates of the cost related to the part of the Intranet that individual managers were most familiar. Isolated instances where costs associated with the Intranet were known included: the budgeted base costs for SXED, the costs of in-house (SXED) application development (tracked through a cost recovery program), the costs of contracted Intranet application or Web site development projects, the costs of corporate assets (hardware and software) used to manage the Intranet, and the full-time equivalent (FTE) allocations to the development and maintenance of some Intranet Web sites. For example:

- SXED application development cost recovery is limited to development and QA resources directly working on the development project. The client is not charged for architecture input, manager time, infrastructure overhead, etc. The 2004 budget estimated the base costs for SXED to be $2.1 million and the cost recovery budget to be $1.3 million.
- Some managers who used external contractors quoted the amount paid for the design and development of their Intranet site.
- Intranet maintenance costs ranged from two FTEs each working half time to maintain the Horizons Intranet site, to an estimate of 20 to 25% of an FTE to maintain a site.

The audit observed that for those Intranet development projects where costs had been tracked, there was often a failure to consider the true cost of ownership (e.g. ongoing maintenance of content, technical upgrades/support, etc.).

Without measures of the cost of ownership for Intranet content, management must define priorities and allocate resources among competing corporate priorities with less than complete information.

Recommended that:

1.3.1   BCD, through the Intranet Steering Committee, implement processes to capture the costs of managing Intranet content.

1.3.2   BCD, through the Intranet Steering Committee, track and regularly review the costs of managing Intranet content and report to the Executive Committee.
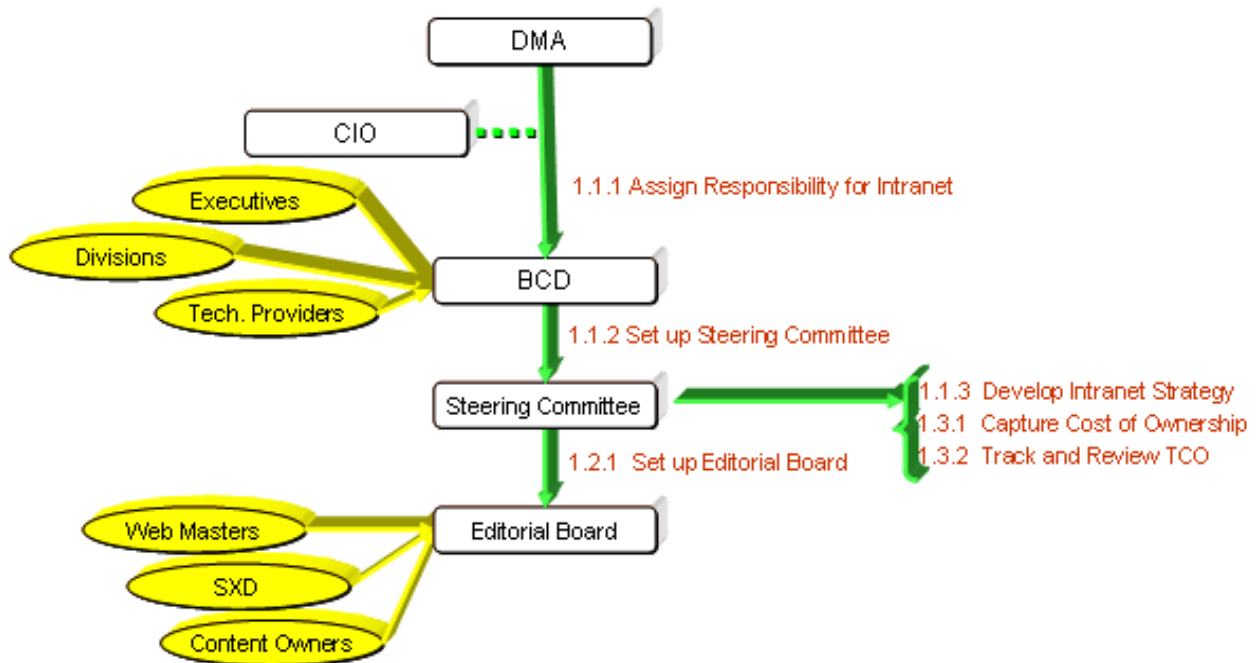
Action and Time Frame

1.3.1   BCD will report on the resources and expenditures that are incurred through the Communications Bureau.

Time Frame: Under way.

1.3.2   The Steering Committee will track the costs to the Communications Bureau for management of the Intranet to BCD and the CIO prior to reporting to Executive Committee.

Time Frame: The first report will be delivered to BCD on April 28, 2006.

Summary of Management Recommendations

2.0 Efficiency and Effectiveness of the Intranet

2.1 The Effectiveness of Intranet Content

User efficiency and effectiveness is diminished due to the existence of FAC Intranet Web sites that contain unwanted content, lack feedback channels and have unfamiliar Web site layouts. Overall, FAC Intranet content is very inefficient to access, resulting in many user complaints and examples of frustration.

Auditees identified the following characteristics of FAC Intranet content as factors which limited user efficiency and effectiveness, and contributed to user frustration:

■ The content of many of the FAC Intranet Web sites is often not aligned with user needs. Many of the FAC Intranet Web sites were described by users as a repository for archived information rather than a tool that is focussed on addressing user needs. Several auditees emphasized the importance of determining what users want from the Intranet, and then verify that what is provided meets user expectations. However, there is no established process for assessing how well the FAC Intranet meets user needs. Without knowledge of levels of user satisfaction, it is difficult for Content Owners to determine how effectively their Intranet Web site meets user needs. An example of desired content included adding more information in the Career Cycle area which currently has a focus on rotational staff.

- Users question the reliability of FAC Intranet content because some content is inaccurate, outdated or contradictory. Many examples of outdated content on the FAC Intranet were observed, including some Intranet sites that referenced Divisions that no longer exist, Ministers who have been replaced and the names of staff who are no longer with the Department.

- Many FAC Intranet sites lack feedback mechanisms that allow users to follow up with questions to content owners. In many cases, it is not clear to whom inaccuracies should be reported or questions asked.

- Although all of the Headquarters-based Intranet Web sites that were audited were available in bilingual format, some non-compliance with the Official Languages Policy was observed on mission Intranet Web sites. Examples from Paris, London and Washington are provided below.

Inaccurate or outdated content may provide users with incorrect information. Scepticism regarding the reliability of FAC Intranet Web sites may cause users to disregard accurate Web sites. The Intranet is ineffective as a self-service tool when users must "go to the source to get the most up-to-date information". The audit did note that the SMD Intranet Web site has a sunset clause for all information that appears in the "what's new" section to ensure that outdated content is removed in a timely manner.

User feedback (e.g., suggestions, error reporting, user questions, etc.) may go unreported when content owners are not identified and feedback channels are not provided.

If common look and feel guidelines are adopted for Intranet Web sites, many content owners request that they not be too prescriptive, thus providing some flexibility in how the site appears. Any standards adopted should address content management, site development and quality management.

a) Content management would include:
- appropriateness of subject matter,
- look and feel,
- co-existence with E-Business applications (i.e. IMS and HRMS),
- potential duplication with other departmental communications media, such as broadcast emails,
- regular content review, and
- retirement of dated content.

b) Site Development includes:
- identifying business needs and user requirements ahead of site development, and
- good development practices.

c) Quality Management would include:
- quality control,
- how to identify and approve exceptions to policies,
- on-going quality improvement, and
- mechanisms for user feedback and measuring satisfaction.

Recommended that:

2.1.1   BCD, through the Intranet Editorial Board, establish clear operational standards for Intranet site content.

2.1.2   BCD, through the Intranet Editorial Board, initiate remediation of existing Intranet sites to new standards. The Editorial Board should acknowledge content owner time and budget constraints when implementing new policies and standards. A phased approach is recommended.

Action and Time Frame

2.1.1   The Intranet Editorial Board will be responsible for the creation and the dissemination of clear operational standards on content to site owners.

Time Frame: Under way.

2.1.2   The Intranet Editorial Board in cooperation with SXED will review the adherence to standards of the content as it is migrated to the redesigned Intranet. Remediation reports will be reviewed and issued to content owners as required.

Time Frame: March 31, 2006.

2.2 The Structure and Usability of the Panorama Web Site

The current form of the main Intranet homepage – the Panorama Web site – (screenshot below) is widely considered to be unstructured, difficult to navigate, unfriendly to users, and largely a duplication of content with broadcast emails. This makes it inefficient and ineffective as a tool for accessing FAC information.

It is critical that the main Intranet homepage be structured so as to allow users to find the information they need quickly. At the time of the audit, the structure of Panorama was not intuitive and the Web site was considered by users to be difficult to navigate. Several examples of time wasted searching for links or information on Panorama were provided, including excessive effort spent searching for corporate guidelines (Also see Section 3.0 "Dead Links, Orphan Pages, Stale Pages").

Users suggested the criteria and priorities of links listed on the main Intranet homepage could be better defined. For example, the prominence of the daily Broadcast message on Panorama's opening screen was challenged because it is information that is repeated in a daily email to all users.

It was frequently stated that the opening page of Panorama is not structured in a way that provides an intuitively user-friendly means to answer questions (e.g., How many staff at a mission?, etc.). Staff want an Intranet that is more client centric and less organizationally structured. For example, including such things as a "Question and Answer" format that provides information on the location of training applications or forms. Currently, the primary Intranet homepage (Panorama) is a collection of links to stand alone Web sites with little integration and linkage across sites.

The Panorama Web site does not follow common Internet protocols related to such features as left navigation (versus the right navigation used by Panorama), and underlined hyperlinks (not underlined in Panorama).

The Department's investment in the FAC Intranet has been marginalized as a result of limited staff awareness of content and sites available. As a result, users do not experience the benefits (effectiveness) that they could from the FAC Intranet. In addition, there is no overall communication plan that addresses the strategy for promoting FAC Intranet content to users.

The layout of the Horizons Web site was widely regarded as efficient and effective. It is structured around how the information will be used rather than the structure of the organization.

For example, the opening menu is based on "Clients", not business lines.
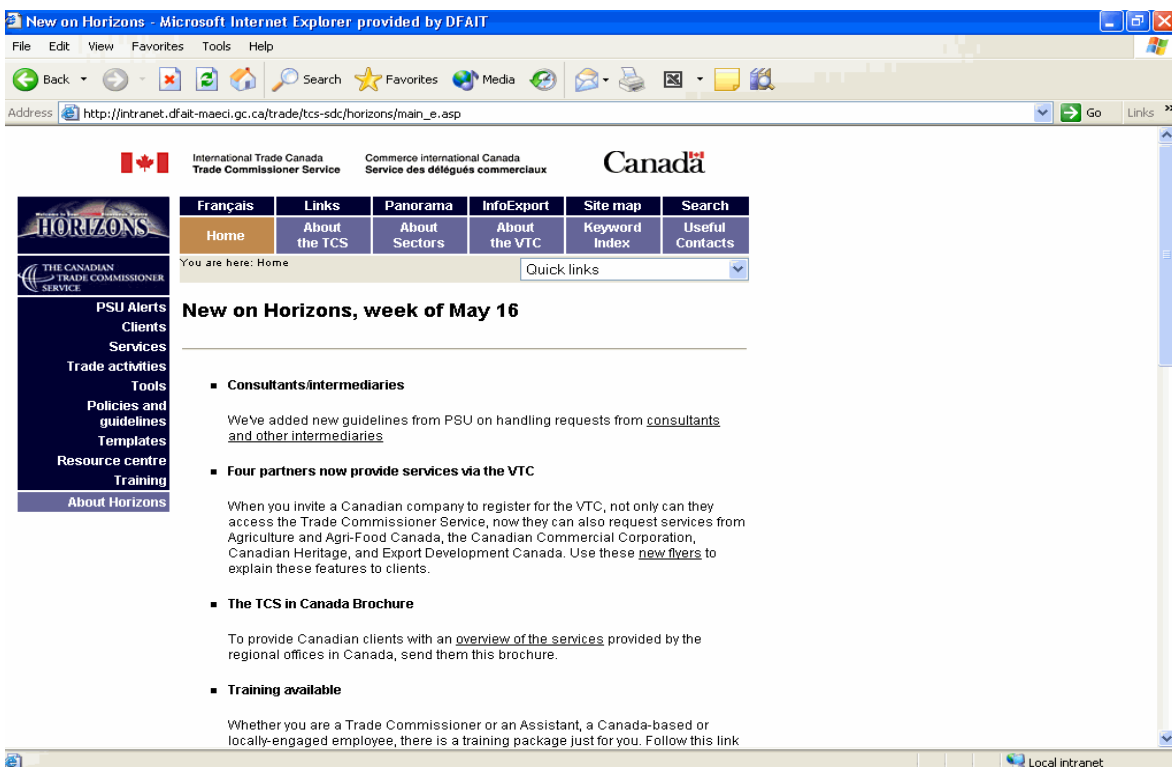
Additional examples of Intranet sites that were suggested as good examples during the audit included:

Recommended that:

2.2.1   DMA define BCD as the owner of the main Intranet homepage.

2.2.2   BCD, through the Intranet Steering Committee, identify owners for all other Intranet Web sites.

2.2.3   BCD, through the Intranet Steering Committee initiate a review of (and overhaul as necessary) all Intranet Web sites to ensure consistency with the new standards.

Action and Time Frame

2.2.1   DMA agrees. The owner of the main Intranet homepage will be BCD as soon as the resources are in place.

Time Frame: Completed September 2005

BCD: Agreed and implemented.

BCD Time Frame: DMA has assigned ownership of the main Intranet homepage to BCD. BCP now manages the main page of the Intranet.

2.2.2   SXEO has provided an up-to-date list of owners of all Intranet applications and content areas.
Time Frame: Completed November 2005.

2.2.3   As indicated in 2.1.2, the Intranet Editorial Board in cooperation with SXED will review the adherence to standards of all Intranet sites as they are migrated to the redesigned Intranet. Remediation reports will be reviewed and issued to content owners as required.
Time Frame: April 2006.

2.3 Effectiveness of the Search Engines

The configuration of Search Engines on the Intranet is ineffective. The Intranet currently has several separate, non-integrated engines that are implemented in an inconsistent manner. The result to the user is slow operation, incorrect results, and overall frustration. This, in turn, leads users to seek their information through less efficient means, such as manual searches, paper searches, or personal contact. This creates the risk that inaccurate search results may lead to decisions based on incomplete or inconsistent information.

Interviewees were adamant that the usability of Intranet content is severely limited by search engines that do not produce accurate results. It was stated that the search engines often do not provide hits where the user knows that a site exists, and searches do not include all of the Intranet Web sites when searching. In the example below, a Travel Expense Claim could not be located by the search engine even though the form is identified on the Intranet.

Factors contributing to ineffective Intranet search engines include:

- considerable Intranet content is disconnected from the scope of search engines;
- the search systems are not effectively managed; and,
- the Intranet architecture is not documented.

Considerable Intranet content is not used because users cannot find it using the search engine. A comprehensive description of the cause of this problem is provided in Section 3.0 of this report ("Dead Links, Orphan Pages, Stale Pages").

To overcome the limited functionality of the search engines, the Horizons Intranet Web site has implemented a key word index. Although not a substitute for an effective search engine, content searchability has improved.

Recommended that:

2.3.1   BCD, through the Intranet Steering Committee, assign responsibility for the common Intranet search engine(s) to SXE.

2.3.2   SXE define, plan, and implement improvements to search engines.

2.3.3   BCD, through the Intranet Editorial Board, ensure that new Intranet Web sites conform to requirements to support searches.

2.3.4   BCD, through the Intranet Editorial Board, initiate documentation and maintenance of the architecture for Intranet content.

Action and Time Frame

2.3.1   BCP on BCD's behalf has communicated the need for a new Search Engine to SXE.
Time Frame: October 2005

2.3.2   As part of its implementation of the Government of Canada's new standard Web Content Management System (WCMS), SXE is developing a solution based on the Verity software.
Time Frame: F/Y 2006/07.

2.3.3   BCD, in accordance with the identified requirements to be supplied by SXE once the new Search Engine has been determined, will ensure that all new Intranet sites conform to requirements to support searches.
Time Frame: Under way FY 2006/2007.

2.3.4   BCD will ensure the documentation and maintenance of the Information Architecture of the Intranet content. SXE will be responsible for the Technical Architecture to support maintenance of the Intranet.
Time Frame: March 31, 2006

2.4 Intranet Application Development Technologies and Environments

There is an opportunity to reduce the costs of development, maintenance, and support of Intranet applications by harmonizing application development technologies, platforms, and environments. For example, Microsoft Java and Sun Java, very similar technologies, are both currently supported.

There are several Intranet applications that replicate functionality already available on the Intranet. For example, auditees reported that there are numerous Grants and Contributions applications within the Department (some web-based, some SQL applications). There are several contact management systems (e.g., Outlook, Contacts Plus, Act 2000, Maximizer, system maintained by ITCan, and some Divisions have their own). Prior to the development of any new Intranet applications, the use of existing Intranet applications should be considered in order to realize lower overall application development and support costs and reduce duplication of redundant Intranet applications.

Standard requirements or guidelines for the technologies used in Intranet applications have not been applied, especially for applications developed outside the Department.

An opportunity to improve collaboration among Divisions was identified by auditees. The suggested goal was to identify best practices, increase reuse of existing applications and reduce re-invention within the Department.

Recommended that:

2.4.1   SXD review and rationalize the platforms and environments for Intranet development and operation.

2.4.2   SXD document and communicate the standards for externally-developed Intranet applications and Web sites.

Action and Time Frame

2.4.1   SXD is moving all Intranet operations to a SIGNET-3 environment, running on a hardware platform built to current SIGNET-3 standards. The upgraded platform will be configured to isolate development, quality assurance and production activities, as recommended by current best practice.

Time Frame: April 2006.

2.4.2   Further to recommendation 2.1.1., SXD will develop operational standards, and support content owners in communicating them to external contractors. FTE resources will be required to be determined.

Time Frame: F/Y 2006/07.

2.5 Availability of Intranet to Missions

Users at some missions have inadequate access to some Intranet content due to limited effective capacity.

Effective capacity is a function of the **network link speed**, the **applications being used**, **user patterns** and the **proper tuning** of applications and network. Capacity constraints have made access to the Intranet and its applications very inefficient for some missions.

Poor Intranet response times are limiting the use of some tools intended to improve productivity. At the time of the audit, the Buenos Aires mission stated that virtually all Intranet applications are "painfully slow, to the point that they are either not used at all or, if used, they take so long that they either time-out, do not function regardless of how persistent the user is, or take so long that it has an enormous negative impact on productivity". For example, accessing a travel expense claim form from the Forms@DFAIT application can take as long as fifteen (15) minutes. Action has been taken by the department to address the difficulties experienced in Buenos Aires; however, these experiences may be similar with other applications and at other missions.

The Vienna, Austria Embassy tried to submit a fifteen (15) line posting to the mission Consular Officer "Community of Practice" run by SXKL using Tomoye software, but the user gave up after it took more than thirty-five (35) minutes to upload the posting. Although Communities of Practice have been established in order to share information and seek support from peers, those at some missions cannot participate due to slow network response times.

Factors that contribute to poor Intranet response times include:

- the effective capacity at some missions is not sufficient to efficiently deliver Intranet applications;
- caching at some missions may be sub-optimal (especially related to forms); and,
- applications, files and forms may be unnecessarily large.

There is the risk that users at missions with limited access to the Intranet or its applications will avoid using the Intranet or revert to unapproved options (e.g., locally saved versions of downloaded documents or outdated information, etc.).

Recommended that:

2.5.1   BCD, through the Intranet Steering Committee, establish minimum standards of performance for all new Intranet applications and Web sites (e.g., minimum response times).

2.5.2   SXD review existing Intranet applications and Web sites to find means of reducing transfers of large files and forms (caching, reducing file size, etc.).

Action and Time Frame

2.5.1   **BCD Response: BCD does not accept responsibility for establishing technical performance standards. SXE, through simulations of low bandwidth locations, should establish the minimum standards to which all Intranet applications and content must conform.**

        Time Frame: n/a.

        ZIV Comments: This response suggests that the recommendation is being interpreted as a technical recommendation. However, the recommendation is for the establishment of <u>user</u> standards or <u>requirements</u>, so that the users can define the performance that they expect. This is the responsibility of BCD through the Steering Committee. It is SXE's responsibility to deliver systems and applications whose performance meets these user standards.

        This comment is being provided as a clarification in order to expedite final issuance of the report.

2.5.2   **SXD Response: New operational procedures to come with the re-designed Intranet will include as an objective the need to reduce transfers of large files. They will be supported by the new Web Content Management System (which should reduce the need for transfers) and improvements in the network (which should ease constraints on transfer).**

        Time Frame: F/Y 2006/07.

2.6 Intranet Security

The lack of controls on material being published on the Intranet has management concerned that sensitive information available on the Intranet individually or collectively compromises security.

During audit interviews, the concern was raised that locally engaged staff with limited security clearance have access to information on the Intranet, such as personal information and property descriptions, that may collectively be sensitive. The audit found that a quality control process was not implemented to ensure that Intranet content was appropriately classified prior to its publication to ensure that it does not compromise security. Although there is general awareness of the importance of security, there is a need to reinforce security with respect to Intranet content.

Quality control criteria for publication to the Intranet, including content security classification procedures, are not defined or implemented. The Department needs to assign responsibilities for training of Intranet publishers on the security policies and procedures for Intranet content.

The audit observed alternatives to the Intranet for the dissemination of potentially sensitive information. For example, some Divisions use shared folders instead of the Intranet for the storage and secure dissemination of potentially sensitive information. Shared folders permit better controls over access to sensitive information than the Intranet.

Recommended that:

2.6.1   BCD, in consultation with IST, identify and assess the adequacy of existing security policies and procedures related to Intranet content.

2.6.2   ZIV conduct a follow-up security audit of Intranet content in six months to identify outstanding security risks.

2.6.3   BCD, in consultation with IST, educate Intranet publishers on the security policies, procedures and quality control measures.

Action and Time Frame

2.6.1   BCD will work with IST to assess the existing security policies and procedures as relating to Intranet content.

Time Frame: March 31, 2006.

2.6.2   The recommended audit was launched by ZIV on November 30, 2005 and will be completed by March 31, 2006.

Time Frame: Under way.

2.6.3   BCD will contact all Intranet publishers to ensure that security policies, procedures and quality control measures are understood.

Time Frame: April 28, 2006.

Summary of Efficiency and Effectiveness Recommendations
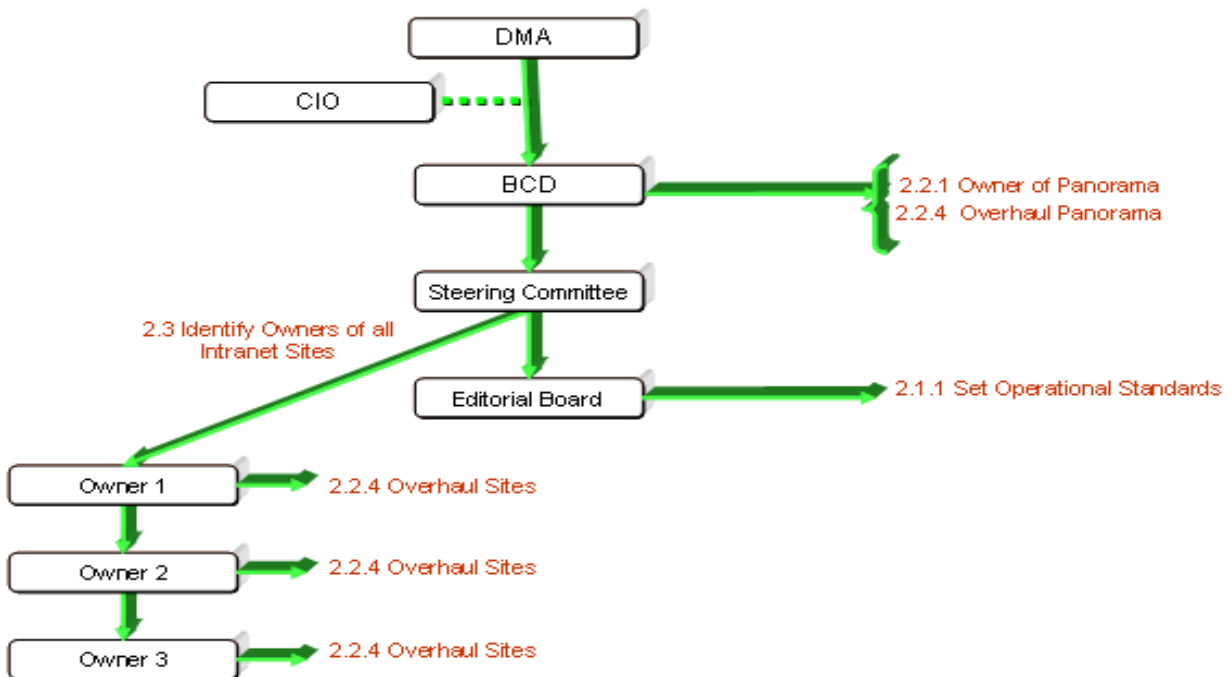
3.0 Meeting Standards for Availability and Integrity

3.1 Dead Links, Orphan Pages, Stale Pages

The integrity of the content of some of the reviewed Web sites is low, which exacerbates the efficiency and effectiveness problems noted elsewhere in this report.

This situation typically indicates that a site has not been maintained in a state of currency. It is evident in the following ways:

- **Dead Links** - This is the case where a hyperlink points to a page that is no longer valid. It arises when a page has been deleted or moved and the hyperlinks that point to that page (being on other pages and sites) are not updated. Dead links waste the time of users attempting to follow logic threads and links.

Examples of dead links were found only two pages deep from the main Panorama homepage: http://intranet/menu-e.asp

and clicking on
Other Directories

and then on
Listing of Mission Security Officers.

This returns an error message: "404 Page Not Found". This is illustrated below.
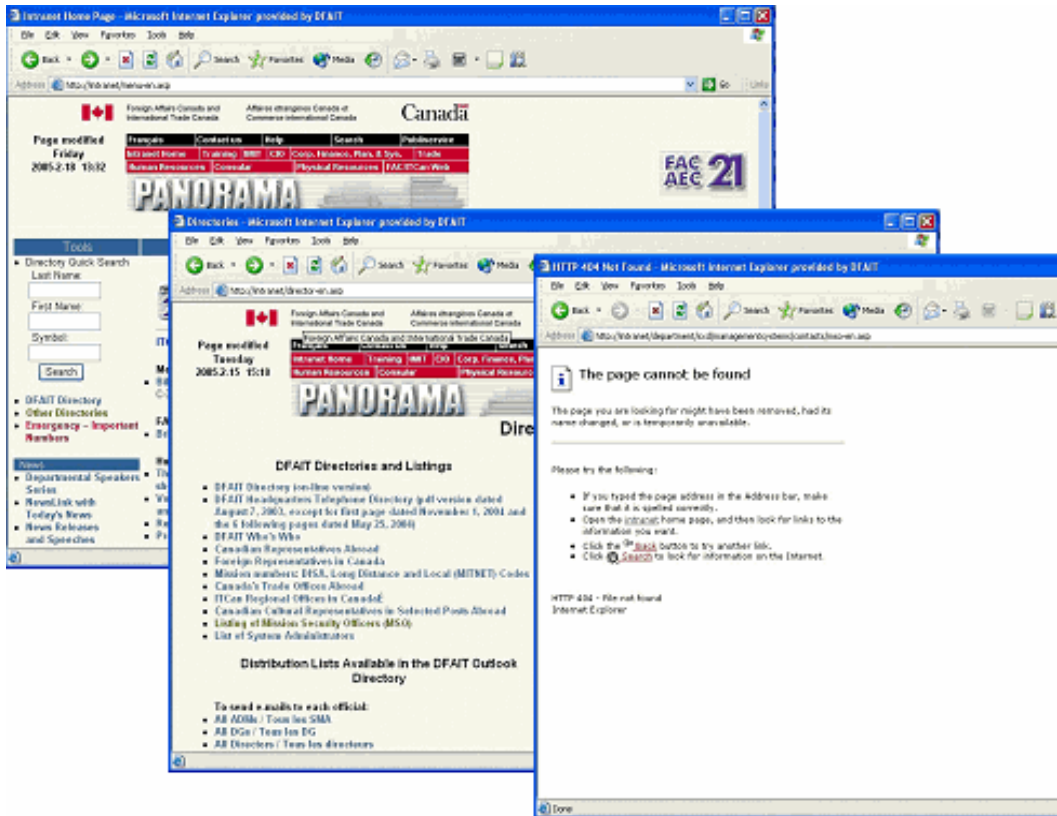
- **Orphan Pages** - This is the case where an HTML page exists on a server, but there is no hyperlink that points to it from any other page on the Web site. As a result, the only way a user can view that page is by explicitly typing the URL (hyperlink address) in the address bar or if the Web site is exposed through a search engine query. Orphan pages arise when a page has been created, but no reference to it has been created on an existing page. Orphan pages also contribute to problems for maintenance and configuration management (version control).

- The Watchfire automated Web site analysis tool uncovered over 100,000 examples of orphan pages. It is acknowledged that many of these pages may be valid files used or generated by the web servers and used internally as part of the server's normal operation. However, it is probable that many of these files are obsolete working versions (e.g. incomplete versions of files in the process of being edited), and that a significant number of them could be removed. This would make maintenance of the content more straightforward. It would also make the results produced by a tool such as Watchfire more meaningful in guiding clean-up operations.

Links to several examples of orphan files are provided here:

http://intranet.dfait-maeci.gc.ca/0616-HRD-NewStructure1.BK1
http://intranet.dfait-maeci.gc.ca/about/descript/menu2-en.asp
http://intranet.dfait-maeci.gc.ca/about/descript/menu2-fr.asp

- **Inaccurate Content** - This is the case where the information provided on a web page is not correct. It may arise when information has changed, but the reference has not been updated, or when information has not been validated between two different references. This makes the web experience ineffective and frustrating for users. User confidence is negatively impacted, often leading to users seeking alternative sources for information.The chart below illustrates the extent of orphan pages residing on the principle Intranet server (lbpis02). Inaccurate content may arise because of a disconnect between the content owner and the Web site publisher or application provider, either in changes that have not been communicated to the publisher or in incorrect information provided to the publisher.

* Pages on
principle Intranet Server (lbpis02)
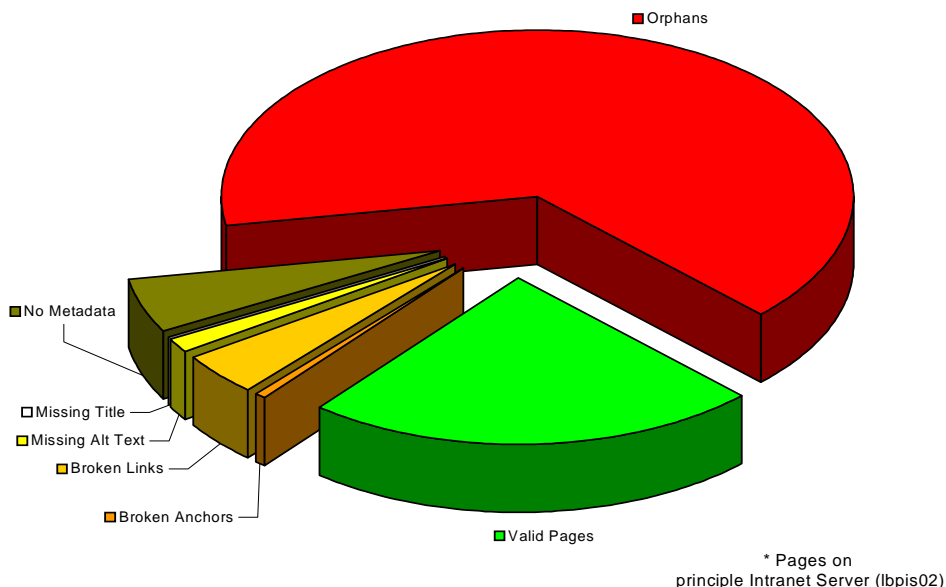
An example, provided below, shows a file that was posted in 1997 and has not been modified since.
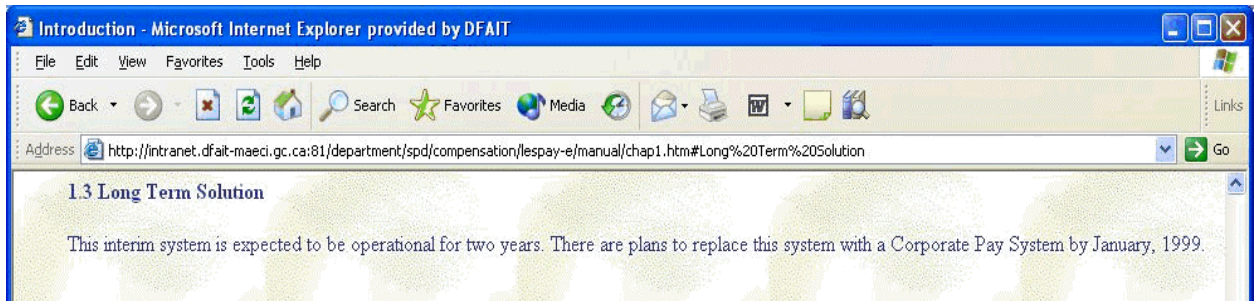
The inventory of 123,705 pages residing on the primary Intranet server (lbpis02) is categorized by the file date in the chart below. The breakdown reveals that more than half of the pages are three or more years old. Although some of the older Intranet pages are maintained for historical or other legitimate reasons, it is likely that many of the older pages are inaccurate and obsolete.

* 123,705 pages on principle Intranet Server (lbpis02)
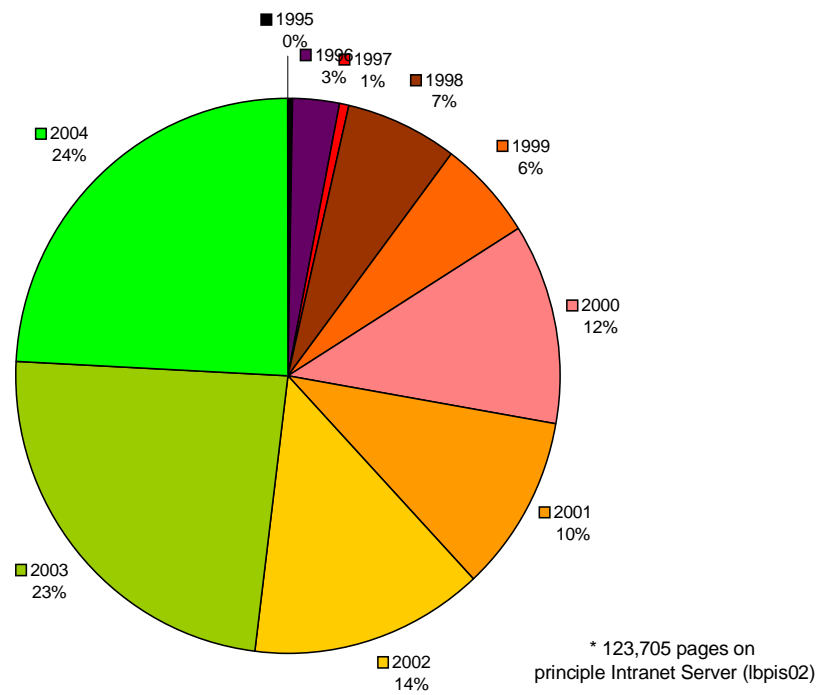
Recommended that:

3.1.1 **SXE review all pages on the principal Intranet servers and remove all dead links and orphan pages.**

3.1.2 **BCD initiate a review by Web site owners of all content for currency and accuracy.**

3.1.3 **SXE, in consultation with content owners, periodically scan all sites in order to identify and remove dead links, orphans, and stale content.**

Action and Time Frame

3.1.1 **SXE has reviewed and identified the dead links and orphan pages on the current Intranet site. As noted in recommendation 2.1.2, only re-usable content, which complies with standards, will be migrated to the redesigned Intranet site.**

Time Frame: April 2006.

3.1.2 **BCD will undertake a review of all Intranet content and contact the respective owners with the results and a recommended action plan. Resource requirements for this task have been addressed in the Intranet Re-design Project.**

Time Frame: February 28, 2006.

3.1.3 **SXE currently offers this as an on-demand service to content owners. The migration to the newly re-designed Intranet site will eliminate the existing problems. The introduction of new standards and processes, supported by a Web Content Management System, should simplify the task of maintaining current and correct content for content owners.**

Time Frame: FY 06/07.

Summary of Standards for Availability and Integrity Recommendations
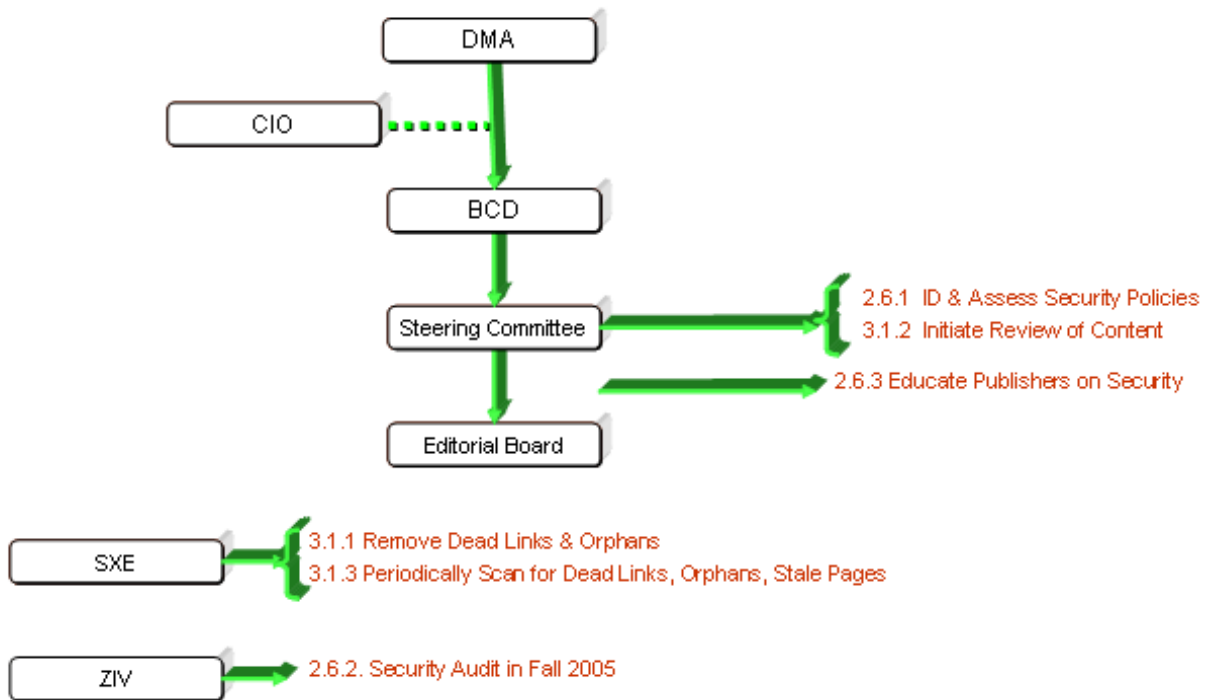
4.0 Best Practices

This section identifies those practices which ZIV considers to be best practices.

4.1 COBIT and ITIL Practices for IT Management

The Intranet should be considered another Information Technology (IT) service and, therefore, should be managed according to IT management best practices. Control Objectives for Information Technology (COBIT) has been developed as a generally applicable and accepted standard for good practices for IT control. COBIT is based on existing Information Systems Audit and Control Foundation (ISACF) Control Objectives enhanced with existing and emerging international technical, professional, regulatory and industry-specific standards. Examples of best practices and further information on COBIT are contained in Appendix C. ITIL (IT Infrastructure Library) is a widely accepted approach to IT Service Management.

4.2 Compliance with the Official Languages Policy

The Headquarters based Intranet Web sites audited were compliant with the Official Languages Policy. The non-compliance to the Official Languages Policy was limited to some mission sites.

4.3 Horizons Intranet Web Site

The management framework of the Horizons Intranet Web site exemplifies several practices recommended in this audit report. For example, the Horizons has clearly communicated that its purpose is to support ITCan personnel in the field with "usable and actionable" content. The

Horizons Intranet site was based on a comprehensive analysis of user needs, and its Intranet Advisory Board regularly reviews performance metrics. A contact person is identified on each Horizons Intranet Web site making it easy for users to ask questions or provide feedback. Processes have been implemented for the ongoing management of new and existing content on the Horizons Intranet, and operational working groups actively manage content to ensure it is usable and accurate. The launch of the Horizons Intranet Web site was accompanied by considerable publicity and education. High levels of user awareness of content increase the likelihood published content will be used, therefore improving the returns on the investment in the Intranet.

Audit Participants

Formal audit interviews were performed with the following participants[4]:

Position	Organization
Head, Publishing Service and Intranet Webmaster	SXE
Trade Commissioner, Overseas Operations	TCS
Deputy Director, Information Organization and Disposition Services	SXKI
Communications Strategist, Office of ADM Human Resources	MSV
Account Manager, Client Liaison and Partnering Division	SXEC
Senior IMT Resource Analyst	SXM
CFSI Webmaster	CFSM
Information Technology Advisor, Management Services Division	XDM
Team Lead (AMS service Desk)	SXEO
Lead Internet/Intranet Web Systems Analyst	
Acting CIO and DG Information Management and Technology Bureau	SXD
Director of Communication Services	BCD
SXE-Client Services	SXEP
Acting Deputy Director, Application Operation	SXEO
Deputy Director, Application Development	SXED
Deputy Director, Modern Management	DMAX
Deputy Director	SXTM
Deputy Director, Overseas Operations	TCS
Web Production Manager	SXEO
Web Coordinator/Internet Content Manager	PEP
Associate Deputy Minister	DMA
Senior Project Officer	IBOC
Human Resources Management System and Compensation Services	SMD
Deputy Director, Foreign Policy and Corporate Communications Division	BCF
Deputy Director, Office of Innovation and Excellence	DMAX
Director, Outreach Programs and e-Communications Division	BCP
Deputy Director, Human Resources Management System and Compensation Services	SMSH
Deputy Director, Corporate Security Division	ISC
Regional eServices Manager, Export Development Division	TCE
Executive Assistant, Headquarters Administration Bureau	SPD
Program Officer, Peacebuilding and Human Security Division	AGP
Policy Advisor, Canada-US Advocacy and Mission Liaison Division	NUR
Systems Administrator, Application Operations Division	SXEO
Director General, Communications Bureau	BCD
Manager, Application Development and Maintenance	SRBI

---

[4]Due to provisions of the Privacy Act, the names of participants have been removed from the final report.

Servers and Sites Covered

Server	URL	Primary Role	SITES						
			Splas	Panorama	Colour	Title	Different	Not Found	Total
lpbis02	http://intranet	Panorama PLUS Others		42	3	4	16	5	70
lbpk01	http://corpapps	EQAMS, PubReg, Directory			1		2		3
	http://hrms-sgrh.dfait-maeci.gc.ca	PeopleSoft					1		1
lbpcat01	http://lbpcat01.capps	CATS, Tech Library					1		1
lbpk06	http://notespub01.dfait-maeci.gc.ca	Competitions, Acq Pol DB					2		2
albertpr	http://srdweb	Property, Materiel, Mail				1			1
lbpkz02 (on Internet)	http://pubx.dfait-maeci.gc.ca	Pubs Catalog			1				1
lpbis04	http://intranetapps	Various Applications	3	0	2		10	2	17
TOTAL									96

Illustration of Intranet Servers:

Intranet Intrastructure - The Servers
Note: Some of those servers could be the same machine

HQ

70 Knowns sites
Http://intranet

lbpis02.lbp.dfait-maeci.gc.ca
Watchfire Report run Here

3 Knowns sites
http://corpapps/

lbpk01.capps.dfait-maeci.gc.ca

1 Known site
https://hrms-sgrh.dfait-maeci.gc.ca/

1 Known site
http://hpux02.lbp/stl.htm &
http://lbpcat01.capps:8090/catsdocs/home.html

lbpcat01.capps.dfait-maeci.gc.ca

2 Known sites
http://notespub01.dfait-maeci.gc.ca/

lbpk06.capps.dfait-maeci.gc.ca

1 Known sites
http://srdweb/default.htm

albertpr.albert..dfait-maeci.gc.ca

1 Known site
http://pubx.dfait-maeci.gc.ca/

lbpkz02.dfait-maeci.gc.ca

17 Known Sites
http://intranetapps/

appserv.dfait-maeci.gc.ca

Missions

Paris
http://

London
http://chuk2/

Tokyo
http://tokyoapp/

New-Dehli
http://delhiapps/

Washington
http://wdc_intranet/

Control Objectives for Information and Related Technology (COBIT)

Control Objectives for Information and related Technology (COBIT) were developed as a generally applicable and accepted standard to ensure that IT has an effective Management Control Framework and is able to meet client and management expectations. COBIT includes existing international technical, professional, regulatory and industry-specific standards and is now recognized by TBS as an applicable framework for the review and audit of information systems in the Government of Canada.
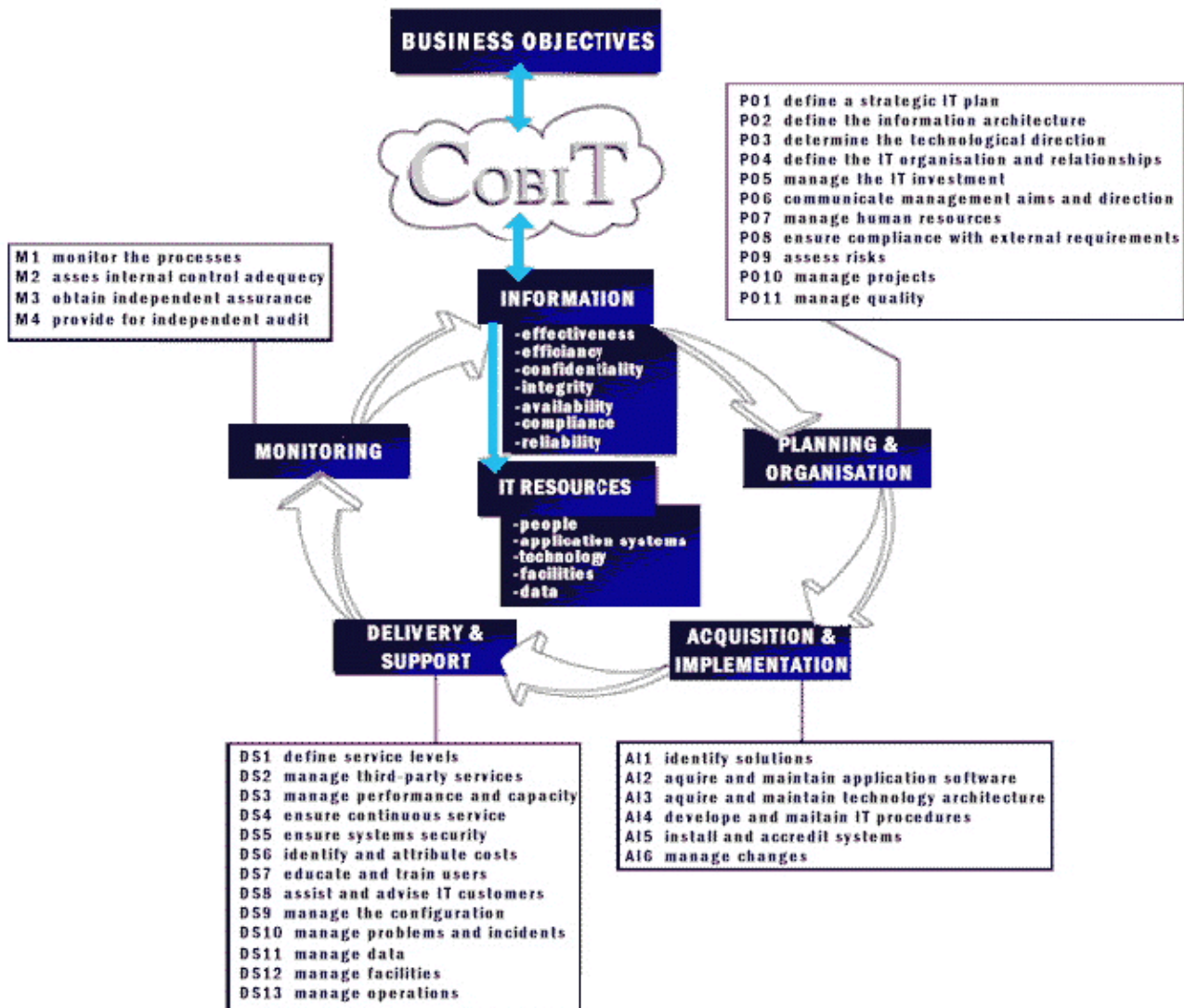
COBIT is designed to be used by three distinct audiences:

- **Management:** to help them balance risk and control investment in an often unpredictable information technology environment. Management needs generally accepted IT governance and control practices to benchmark their existing and planned IT environment. COBIT is a tool that allows managers to communicate competing requirements and bridge the gap between control requirements, technical issues and business risks.

- **Users (i.e. Business Process Owners):** to obtain assurance on the security and controls of information technology services provided by internal or third parties.

- **Information systems auditors:** to substantiate their opinions to management on internal controls.

The COBIT methodology indicates that there are a number of different processes consisting of many controls, and there is a systematic way to assess those controls.

COBIT consists of a framework for control in IT based on business information criteria and documented by control objectives organized by IT domains, processes and activities. Each of these areas has in addition to a set of control objectives, a definition and a rationale for control.

Business orientation is the main theme of COBIT. It is designed not only to be employed by users and auditors, but also, and more importantly, as a comprehensive checklist for business process owners. Business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. This includes providing adequate controls. COBIT provides a tool for the business process owner that facilitates the discharge of this responsibility.

The COBIT framework starts from a simple premise: *In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes*. The domains are identified using wording that management would use in the day-to-day activities of the organisation.

- **Planning and Organizing** - This domain covers the strategy and tactics related to the identification of the way information technology can best contribute to the achievement of the business objectives.
- **Acquisition and Implementation** - To realise the IT strategy, IT solutions need to be identified, developed or acquired as well as implemented and integrated into the business process.
- **Delivery and Support** - This domain is concerned with the actual delivery of required services, ranging from traditional operations over security and continuity aspects to training. In order to deliver services the necessary support processes must be set up.
- **Monitor the Process** - All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

For further information on COBIT see http://www.isaca.org.

Audit Areas:				
Governance and overall management framework	*Satisfaction of user and business requirements*	*Ongoing costs of ownership*	*Accuracy and currency of content*	*Availability and integrity of systems*
COBIT Explanation:				
IT Governance refers to a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.	User satisfaction is measured by: ▪ Effectiveness ▪ Efficiency ▪ Confidentiality ▪ Integrity ▪ Availability ▪ Compliance ▪ Reliability of information. Business requirements refers to the degree of compliance to stated or implied parameters and specifications.	Determination of how costs of ownership are monitored, and the process for comparison of actuals to budgets.	Information is correct and up to date.	Information is usable on demand to support business functions, and the information is accurate and complete.

Glossary

Accessibility Check
An accessibility check is a test that is performed to determine the compliance of a web page against a checkpoint. Each checkpoint may comprise more than one check to test for compliance.

Application
An application that is part of the content of a Web site that is dynamically produced by a server-side application technology (which is not to be confused with an application server). From a security perspective, each page that is dynamically generated is an application. Note that applications may also be nested. For instance, the collection of ASP pages that make up WebXM can be considered to be the application 'WebXM'.

Application Server
A server that awaits various types of requests (depending on the type of application server) and provides the business logic to process those requests.

Authentication Point
A content asset that either contains an authenticator (in the case of form-based authentication) or that was accessed by means of an authenticator.

Authenticator
In the case of form-based authentication, the authenticator is the application that validates a user's credentials. HTTP, NTLM, and certificate-based validation all use authenticators that are inherent to the web server.

Availability
Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

Boolean Expression
Boolean expressions are often encountered when doing searches on the web. In Boolean searching, you can use an AND operator between two words to find documents that contain both the words, or you can use an OR operator to find documents that contain either one of the words.

Broken Links Error Types
A Broken Links report includes the following error types:

- File Not Found: Occurs when a URL points to a file on the server that does not exist, and is usually caused by misspelling of the URL or when the target file has been deleted or renamed.
- Cannot Connect: Occurs when the target server does not respond to the request from the browser, and is often due to a server that is down or too busy.
- Host Not Found: Occurs when a URL points to a server that does not exist.

- Time-out: Occurs when an existing server responds but does not return the data fast enough and the browser times out.
- Other: Occur when there is unauthorized access or when someone is unable to open the file. If the error does not fit within one of the existing error types, it is included in the Other error type.

Certificate

A certificate is an electronic 'credit card' that establishes your credentials when doing business or other transactions on the Web. It is a public key that is signed (using a digital signature) by a certificate authority (CA). Certificates also include some other ancillary attributes, such as the name, serial number, and expiration dates.

Certificate Authority

A CA is an authority in a network that issues and manages cryptographic credentials and public keys for message encryption. It is a part of a public key infrastructure (PKI).

Context

Many reports display contextual information about an issue found during a scan. Context is the information about an issue that is captured during the scan. For example, in the HTML anchor <A HREF = "brokenlink.htm">Broken Link</A>, the context is the text between the <A> and </A> tags. Other link contexts include JavaScript, Flash, Image Map, Image, Style Sheet, and Real Media.

Dashboard

A dashboard is a set of properties that defines how My Watchfire and My Watchfire Classic looks and behaves. In the case of My Watchfire, properties include which issues are presented, how issues are grouped and named, how scores are presented visually, and how its reports behave. In the case of My Watchfire Classic, properties include which issues are presented and how scores are calculated.

Digital Signature

A digital signature is a signature derived from the content of a message that can be used to prove the integrity and origin of that message.

Document

A file that contains content relevant to the goals of a Web site.

Domain

A domain is the part of the Uniform Resource Locator (URL) that locates an organization or entity on the Internet; for example, www.watchfire.com.

Domain Name

A name that identifies one or more IP addresses and consists of at least a top-level portion, such as .com, .gov, .edu, or .net, and a second-level portion, such as Watchfire or MicroSoft. A third, fourth, or more level portions may need to be added to it (for example, support.company.com).

Domain Name Service

A domain name service (DNS) resolves domain names to their associated IP address.

Effectiveness
Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency
Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.

Encryption Method
The process by which data is encrypted and decrypted. For example, data encryption security (DES) is an encryption method.

External Domain
External domains are those domains that have a different URL (up to the first backslash) from the URL of the site being scanned. If www.watchfire.com is scanned, domains such as www.products.watchfire.com will be considered external domains in the reports. This also applies to third-party reports in that URLs that are considered third-party are those that are external to the scan.

File
Anything stored on a disk that is understood as a file by the operating system of the computer housing the disk.

Host
A computer on a network. Each host can be located based on its IP address, or by a fully qualified domain name. If the host is referred to by its host name, that name must first be resolved to an IP address by a Domain Name Service before the host can actually be located.

Host Name
The name of a host with respect to its Intranet. Relative to an extranet, a host is named using a fully qualified domain name.

Image Description
A description of the content of an image, used by people who cannot view or process the image fully. If the image is also described in text accompanying the image, or is a simple icon adequately represented by the ALT text, a separate description may not be necessary.

Integrity
Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Internet Protocol Address
An Internet Protocol (IP) address is a numeric identifier for a host, for example, 293.26.1.19.

Internal Domain
A domain that is included in the content scan and that appears in the Starting URLs list.

Key
In cryptography, a key is a constant value that is applied using an algorithm to a string or block of unencrypted data to produce encrypted data, or to decrypt encrypted data. Although there

are billions of keys in existence, a piece of data that was encrypted with one key can only be decrypted using that same key (or a related key).

Key Exchange Protocol
A protocol governing how two parties exchange keys to use in securing a transaction. Once keys have been exchanged, data can be encrypted at the sender's end (using an agreed-upon encryption method) and decrypted at the receiver's end.

Key Length
Key length is a measure of the size of the data that makes up a key, and hence determines how robust the key is. Longer keys, such as 128 bit, are generally considered to be harder to crack than shorter keys (48 bit).

Link
An HTML element that allows a user agent to navigate from their current location to some URL. Links are URLs that can be clicked.

Method, Web Server
A way that a web server can manipulate information. Some methods are dangerous because they allow remote users to affect data on the web server.

Navigation Trail or 'You Are Here'
The navigation trail, also known as 'You are here', shows the path through the WebXM Control Center from where you started to where you are now. If there is not enough space to display the entire path, ellipses appear at the beginning of the path.

Page
A page is a web document that can be experienced by a user. A page can include file types such as HTML, Active Server Pages, Java Server Pages, Microsoft Office, Adobe Acrobat (.pdf), Real Networks Streaming Media, Windows Media Player , XML , Macromedia Flash, or Javascript.

Port
A numerical location on a host on which a server awaits requests. For instance, a host may receive requests on ports 80 and 443. Since the web server on that host awaits requests, or 'listens' on port 80, and the application server on that host listens on port 443, requests made to those ports will go to their respective servers. Requests made to ports on which no server is listening will not be honoured.

Private Key
A private key is an encryption key known only by a select group of clients. Private keys can be used in conjunction with a related public key (in which case the public and private keys are asymmetric) or by themselves (in which case they are symmetric) to effectively encrypt messages and digital signatures.

Public Key
A public key is the part of a public-private key pair that is made available to anyone to validate data encrypted with the private key. Because public keys are always part of a key pair, they are by nature asymmetric.

Public Key Infrastructure
A public key infrastructure (PKI) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Publish a Survey
When a Feedback survey is published to a Web site, HTML and .jsp pages are generated and saved to the Feedback Server. In addition, the survey's status is changed to active, meaning that it is available to Web site users.

Reliability
Reliability of information relates to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting responsibilities.

Secure Sockets Layer
The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet, that has been succeeded by Transport Layer Security (TLS). SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The 'sockets' part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

Secure Sockets Layer Server
A server that handles SSL HTTP requests.

Server
A program that resides on a host and waits for and fulfils requests from other hosts. Servers receive requests through one or more ports on a host.

Server-Side Application Technology
A technology that is enabled for a web server, such as Active Server Pages (ASP), Java Server Pages (JSP) or PHP. Server-side application technologies produce dynamic web content, which is considered to be an application.

Style Sheet
A set of formatting or style commands that are kept separate from the actual content of a web page. This makes formatting easier as it can be defined globally, rather than each time a particular element occurs.

Symmetric Key
The type of key used in a form of encryption where the same key used to encrypt data is needed to decrypt it.

Transport Layer Protocol
Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet and is the successor to the Secure Sockets Layer (SSL). When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message.

URL
A URL, or Unique Resource Locator, is a way of indicating the location of an item in cyberspace.

User Type
A user type, and there are four of them, describes a particular user's abilities within the WebXM Control Center. However, their capabilities can further be extended by the role or roles they assume under webspaces. The four user types are: Standard User, System Administrator, No Access, and Webspace Creator.

Web Server
A server that awaits Hypertext Transfer Protocol (HTTP) requests, and serves up HTTP in response.

Web Site Technology
Technology assets, such as a content management system, that are used to build and manage the content assets of a Web site.