**RAPPORT DE MISSION**

**Evaluation Mi-Parcours du Projet de mise en Place d’une Solution Intégrée de Gestion Electronique de Documents, Archivage Numérique et des Archivages Physiques**

***Audite Réalisé au Troisième Trimestre 2018***

***Par NYCOSOFT UG,***

**Content**

[**1-** **Introduction** 2](#_Toc525295557)

[**Objectifs de l’évaluation** 4](#_Toc525295558)

[**Guide de Notation** 4](#_Toc525295559)

[**2-** **Observations & Recommendations** 5](#_Toc525295560)

[**Functional specification Review** 5](#_Toc525295561)

[**Basic document building Workflow** 5](#_Toc525295562)

[**Documents Approval Workflows** 5](#_Toc525295563)

[**Annotation & Notification** 5](#_Toc525295564)

[**Implementation & utilisation** 8](#_Toc525295565)

[**Gouvernance** 9](#_Toc525295566)

[**Annex 1—Elements of an IM/IT governance framework** 9](#_Toc525295567)

[**3-** **Conclusion** 11](#_Toc525295568)

[**4-** **A propos de L’Evaluation** 12](#_Toc525295569)

[**Objectives** 12](#_Toc525295570)

[**Scope** 12](#_Toc525295571)

[**Application Features Evaluation Criteria** 12](#_Toc525295572)

[Audit Capabilities 13](#_Toc525295573)

[**Workflow Process** 13](#_Toc525295574)

[**Extended Features** 14](#_Toc525295575)

[**Application Performance** 14](#_Toc525295576)

[**Application Maintainability** 14](#_Toc525295577)

[**Project Governance** 14](#_Toc525295578)

[**ROI Return On Investment** 14](#_Toc525295579)

[**Note Gobal des évaluations** 14](#_Toc525295580)

[**5-** **Appendix** 16](#_Toc525295581)

1. **Introduction**

**1.** The Office of the Auditor General (the Office) is obliged to respect information management policy objectives of the Treasury Board of Canada Secretariat (the Secretariat) as well as the Directive on Recordkeeping when it comes to corporate information. To meet these requirements, Office personnel must use the Office’s electronic document and records management system (EDRMS) consistently, and information is to be easily stored, secured, and made available to support operational and strategic activities. According to the Government of Canada Policy on Information Management, deputy heads are responsible for the following, among other things:

* ensuring that departmental programs and services integrate information management requirements into development, implementation, evaluation, and reporting activities;
* ensuring that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of the evolution of policies and programs, and allow for independent evaluation, audit, and review;
* ensuring that information is shared within and across departments to the greatest extent possible, while respecting security and privacy requirements; and
* establishing, measuring, and reporting on a departmental program or strategy for the improvement of the management of information.

**2.** The Secretariat’s Standard for EDRMS states: “Information resources of business value are strategic assets used across government to support effective decision making and facilitate ongoing operations and the delivery of programs and services. The Directive on Recordkeeping requires departments to establish the mechanisms and tools to support the departmental recordkeeping requirements throughout the information life cycle.”

**3.** As an Officer of Parliament, the Office has special authority to operate independently. At the same time, it must meet important government policy obligations. The Directive on Recordkeeping contains many policy requirements for deputy heads. Departments were supposed to meet these obligations by March 2014, but based on feedback from departments and agencies, the Secretariat revised the date to 31 March 2015 to provide the time needed to implement all the requirements. Departments were expected to obtain an accurate and reliable overview of the current level of recordkeeping maturity, identify recordkeeping gaps and weaknesses, and measure recordkeeping progress over time.

**4.** To meet these and other policy objectives, the Office has made a significant investment in electronic document management systems. The Office uses two primary and distinct systems to manage information. TeamMate is specific to audit records and supports the audit process. PROxI is a mission-critical EDRMS that the Office defines as “an integrated suite of tools that will simplify information management, storage, retrieval, and promote the sharing of information across the Office.” PROxI was fully deployed in June 2009.

**5.** The Office received an updated Records Disposition Authority from Library and Archives Canada (LAC) in May 2013. This authority allows the Office to dispose of specific types of information. The authority also requires the Office to properly classify information and record decisions. The Office must continue to track specific types of information—such as information about management and oversight of the Office—and provide it to LAC. This includes senior management decisions outside the scope of a specific audit. PROxI exists to support the management of this type of information.

**6.** The Office now needs to assess the extent to which it has put its information management/information technology (IM/IT) systems into effect to meet IM policies and regulations in practice.

**Objectifs de l’évaluation**

**7.** Nous avons examiné le projet GED sous l’aspects du gap existant entre ;

1. Les exigences fondamentales formulées dans son cahier de charge par AFRILANDFIRSTBANK notamment ;

* Les besoins fonctionnels,
* Les besoins techniques
* Les besoins de gouvernance de la réalisation et de la durabilité de la solution implémentée

Et

B- l’aptitude de la solution actuelle implémentée à répondre aux besoins précisés par le document des spécifications détaillées proposé par le fournisseur de service AYD

De cet examen découlent donc les recommandations que nous proposons dans ce rapport afin de minimiser, voir éliminer le gap constaté.

**Guide de Notation**

La conduite de l’évaluation qui a produit les résultats du rapport repose sur un ensemble de valeurs d’appréciations résumés dans le tableau ci-après. Ces valeurs sont assignées aux performances résultantes des éléments de solutions implémentés pour répondre aux besoins du client

|  |  |  |
| --- | --- | --- |
| Découverte | Definition/Impact | Action/Mitigation |
| **CONFORMITE** | Conformité veut dire adhérence à l’exigences. L’attribution de cette valeur sous-entend que la solution implémentée répond au besoin spécifier. Ce qui implique que la preuve d’évidence est documentée et disponible pour vérification. | Passer au prochain besoin ou indicateurs à vérifier. |
| **OPPORUITE**  **D’AMELIORERATION** | Un Risk faible offrant une opportunité d’amélioration. Unresolved OFIs may degrade over time to become non-compliant. | Review and implement actions to improve the process(s). Monitor trends/indicators to determine if improvement was achieved. |
| **N/C MINEUR** | Un Risk moyen, une non-conformité mineure qui résulte à une déviation des attentes du besoin fonctionnel ou du procès | Investigate root cause(s) and implement corrective action by next reporting period or next scheduled audit. |
| **N/C MAJEUR** | Un haut Risk, une non-conformité majeure qui impacte la fonctionnalité et résulte à une non-conformité de la solution globale | Implémentation immédiate d’une action corrective, analyser la cause mère et appliquer l’action corrective. Re-auditer dans prochaine version pour une re vérification de correction. |

1. **Observations & Recommendations**

**Functional specification Review**

**Basic document building Workflow**

**8.** The fundamental elements of document management are missing, notably,

- The different document types that will be handle by the system, the detailed specifications tend more to refer on processes than focusing on the key objects being processed which should be the document itself.

- Because the types of document are not defined it appears very unclear to determine the lifecycle of each document in the system

- And due to the lac of a lifecycle that defines each single possible state of a document, it is not possible to define any document policy which will clarify the access wright to ach document.

The consequences of the missing definition is a mismatch of business functional profiles and document manipulation roles along the process flow.

In other word we have many substitute roles when we move from one process to another this can definitely lead to a confusion of roles in the document access security., specially in case a single user should act in more than one process in the same system.

**9.** We conducted a review of available metrics to determine whether the Office has put in place procedures consistent with good practices to monitor the implementation of its electronic document and records management system. We requested any and all metrics identifying system utilization that could demonstrate that the procedures in place were consistent with good IM practices.

**Documents Approval Workflows**

**8.** **Credit Process:** of information management (IM) allows an organization to determine whether it knows which documents serve a business purpose, which documents can and should be disposed of, and which documents should be retained due to their enduring value.

**9.** **Complains Process**: review of available metrics to determine whether the Office has put in place procedures consistent with good practices to monitor the implementation of its electronic document and records management system. We requested any and all metrics identifying system utilization that could demonstrate that the procedures in place were consistent with good IM practices.

**Annotation & Notification**

**8.** Effective monitoring of information management (IM) allows an organization to determine whether it knows which documents serve a business purpose, which documents can and should be disposed of, and which documents should be retained due to their enduring value.

**9.** We conducted a review of available metrics to determine whether the Office has put in place procedures consistent with good practices to monitor the implementation of its electronic document and records management system. We requested any and all metrics identifying system utilization that could demonstrate that the procedures in place were consistent with good IM practices.

**Monitoring is not being done as a repeatable business process**

**10.** We found that monitoring is not being done as a repeatable business process, but rather on an ad hoc or transactional basis. This monitoring is limited to how many documents were saved, which groups saved to PROxI, and similar high-level metrics. We saw no summary or analysis document that would enable a reader to comprehend the data provided. In fact, we were advised that the numbers needed to be interpreted carefully and that someone would have to explain their significance.

**11.** The Office of the Auditor General IT Security Policy and the Treasury Board of Canada Secretariat (the Secretariat) Policy on Government Security require monitoring to determine whether the departmental security program is effective. In the Office’s implementation, employees are permitted to store documents that are classified up to and including Protected B in the PROxI repository. Any repositories other than PROxI have the same information storage requirement. We observed that no monitoring has taken place to ensure that no information above Protected B resides within PROxI or the other repositories that Office employees can currently use.

**12.** Employees store documents in repositories other than PROxI. We observed that other repositories continue to be used in the Office: namely, the C:, H:, I:, O:, and S: (read-only) drives. While valid reasons exist for a need for additional storage, such as non-compatibility with PROxI, some of these documents should be stored in PROxI.

**13.** Government policy requires that a mechanism be in place to support recordkeeping requirements throughout the life cycle of a document, including disposal. Also, there is a requirement that information be shared within the Office. Effective sharing of information is based on access, location of information, naming conventions, and search capabilities. Without a consistent approach to profiling electronic objects within PROxI, the IM team may not be able to apply automated disposition activities to dispose of documents.

**14.** In our opinion, monitoring the use of the PROxI system and other repositories would allow the IM team to

* confirm the effectiveness of the system;
* identify the nature and extent of training needed; and
* identify desirable changes to policies, guidance, and manuals.

As improvements are noted, ongoing monitoring can be revised to target particular areas of concern.

**15. In summary.** We found that given the lack of monitoring, the Office does not have assurance regarding the appropriate use of and controls for PROxI.

**16. Recommendation.** The Office should implement monitoring as a repeatable business process to obtain assurance that the electronic document and records management system is being used as intended and is fulfilling the Office’s obligations for records management. Monitoring should consider such things as access rights, location of information, naming conventions, security level, and capacity.

***Management response.*** *Agreed. The information management team has developed a standard monitoring plan that, at a minimum, includes access rights, document classification, naming conventions, and security level. It examines PROxI usage from different facets (for example, the file plan or group usage) and will be repeated no less than annually. The monitoring plan development has been completed, and monitoring has begun. If any new items arise that need to be consistently monitored, they will be added to this plan. The activity Monitoring has been added under the Knowledge and Information Management function in PROxI so that in future, all documentation of monitoring will be captured under a single place in the file plan. In addition, the Access to Information and Privacy (ATIP) Coordinator will periodically monitor the system to ensure that personal information is not being inadvertently exposed. System-generated reports will be reviewed for usefulness and accuracy, and modifications made as needed.*

**No evidence indicates that senior management is receiving information for oversight**

**17.** Providing senior management with periodic reports on the results of key metrics enables management to assess whether the electronic document and records management system (EDRMS) is being used effectively and whether the Office is meeting its IM policy requirements. Because these reports become the basis for sound decision making, we expected to find that they are presented to the Office’s senior management on a regular basis.

**18.** We found no evidence that any monitoring results were presented to the Chief Information Officer (CIO), the Assistant Auditor General of Corporate Services, or the Executive Committee. We reviewed and analyzed interview responses, email responses, the Office’s INTRAnet site, and documents provided by the Office’s IM and information technology (IT) group, but found no documents in support of this audit question. In the absence of briefings, reports, and recommendations to the Office’s senior management, it is unclear how the Office is meeting its legislative responsibilities in relation to Government of Canada policies, standards, guidelines, and directives.

**19.** Our concerns relate to two levels of senior management: the CIO, who has direct responsibility for information management, and the Executive Committee or other body that has responsibility for general oversight. For example, the Executive Committee is responsible for, among other things, establishing policies and principles for managing people and products, and for determining the allocation of resources. To perform these two responsibilities, it must be informed. Monitoring reports would support this need. The CIO has many responsibilities related to IM. Also, the CIO’s strategic plan identifies a vision, a mission, and goals. Without monitoring, the CIO lacks tangible evidence that IM is in line with policy and Office objectives.

**20. In summary.** We found that monitoring results have not been presented to senior management to allow decisions and decision-making processes to be accounted for and supported, in keeping with policy requirements.

**21. Recommendation.** The Office senior management should receive ongoing monitoring reports and analysis that explain whether and how the Office is meeting its information management (IM) requirements. These monitoring reports should be used to assist in making decisions pertaining to any required changes to IM policies and system revisions.

***Management response.*** *Agreed. The information management team will submit a monthly report to the Chief Information Officer and to the Chief Financial Officer, who is a member of the executive team. The report will include statistics on PROxI usage and a summary of the month’s monitoring activities.*

**Implementation & utilisation**

**22.** PROxI was and is intended to be the repository of all records of business value. Fundamental characteristics of a strong electronic document and records management system (EDRMS) include ownership, filing and description, organization, access and protection, storage and retention, and disposal. In addition to meeting the technical requirements of the system, how it was set up and how it is being used greatly affect all of these key characteristics. We expected to see evidence that the Office had analyzed whether the implementation and ongoing use of PROxI needed improvement.

**23.** We reviewed and analyzed documents provided by the Office information management (IM) and information technology (IT) groups to determine whether any gaps in PROxI implementation had been identified. We also interviewed key IT/IM staff and received email responses to specific questions.

**Shortcomings exist in the implementation and use of PROxI**

**24.** We found that formal measurement of progress, as well as user engagement and feedback activities, was done in 2010 as part of an annual review of PROxI. In 2012, another smaller analysis was conducted. Since 2012, no further user consultation or feedback sessions have taken place.

**25.** The 2010 report identified that, among other things, the following areas required attention: access rights and the need for monitoring to better understand user challenges. The 2012 analysis called for a comprehensive review of the Office’s information architecture. Both reviews identified usage concerns and the need for additional training to support better implementation.

**26.** We found no evidence to identify actions taken in response to these analyses. As noted earlier in this report, no regular monitoring activities are in place. We found no comprehensive review of the information architecture, as recommended in 2012. We saw no evidence of changes to course content, as recommended in 2010. While training is available for new employees, it is not mandatory.

**27.** An implementation gap identified by internal audit is the use of unmanaged repositories, which continue to be used even though PROxI has been in place for over five years. At present, an Office-specific plan that would consider business requirements and user functionality enhancements does not exist. Instead of Office-specific solutions, the Office is relying on vendor-supplied technical solutions.

**28. In summary.** We found that there are gaps in the PROxI system use and implementation.

**29. Recommendation.** The Office should conduct a review to identify gaps in current PROxI use and also in the document repository. Improvements should be identified and should be linked to measures so that ongoing monitoring can be conducted to demonstrate progress.

***Management response.*** *Agreed.*

* *The monitoring process that has been recently implemented will identify areas of the file plan requiring modifications.*
* *A review similar to the one carried out in 2010 should be conducted; given the information management (IM) team’s priorities for 2014, this review may not be done until 2015.*
* *The IM team is aware of gaps in IM awareness and will embark on a campaign to ensure that all employees are aware of their responsibilities and have the tools to fulfill them.*
* *With the I: drive under control and managed, the IM team will start a review of the O: and S: drives. The business needs to use alternate drives will be substantiated and documented, so that they could be considered in future system improvements.*

**Gouvernance**

**30.** According to *Optimum: The Journal of Public Sector Management*, “the goal of effective IM/IT Governance is to ensure that all IM/IT initiatives have been managed from an organization-wide perspective and that they contribute to the institution’s strategic business goals.” This journal also defines three elements in an information management and information technology (IM/IT) governance framework ([Exhibit 1](http://www.oag-bvg.gc.ca/internet/English/acc_rpt_e_39941.html#ex1)).

**Annex 1—Elements of an IM/IT governance framework**

|  |  |
| --- | --- |
| **Governance principles** | The principles by which all IM/IT initiatives will be governed. |
| **Governance structure** | The roles and responsibilities of the major stakeholder in the IM/IT governance decision-making process, including committees and organizational elements at the branch level. |
| **Governance process** | The various stages required to review, assess and approve or reject new IM/IT initiatives. |

Source: *Optimum: The Journal of Public Sector Management*, Vol. 29, Nos. 2/3.

**31.** We examined whether an adequate governance structure exists for the IM function and system implementation. We reviewed and analyzed documents provided by the Office IM and IT groups. Also, we received email responses to specific questions and searched the Office INTRAnet for policies to supplement the information we received.

**A weak governance structure exists**

**32.** We found that there is a lack of precision regarding roles, responsibilities, and expectations for the frequency and timeliness of governance activities. The IM policies contained within the policy suite were approved in 2009 and were to have been reviewed in 2011, but this review was not done. Few roles are identified through policies or job descriptions, making it difficult to determine who is tasked with which responsibilities.

**33.** The policy suite available to employees through the corporate INTRAnet site is limited. No specific policy instruments outline internal controls, roles, standards, policies, guidelines, directives, and best practices for the entire IM program. Items such as metadata, social networks, and email, for example, require documented procedures, standards, and guidelines. Likewise, roles and responsibilities for key activities such as system monitoring are not clearly identified. The risk is that when activities are not clearly documented, they may not take place, or may take place in a manner that is not consistent with the expectations of senior management.

**34.** The INTRAnet information in IM and PROxI Best Practices within the IM policy suite is a good foundation and reference point for users. However, the guidance requires more context and is outdated. As an example, the IM Do’s and Don’ts section does not include any rationale for the guidance and does not outline the potential consequence for not adhering to corporate guidelines. It appears that this INTRAnet page was last modified in 2010.

**35. In summary.** We found that the IM policy suite and governance framework is insufficient to achieve mature and sustainable corporate IM systems.

**36. Recommendation.** The Office should update its information management policies and create job descriptions to identify clear roles and responsibilities, set expectations of employees that link to the policy requirements, and establish timelines for updating these policies. A mechanism should be included to ensure that the Office is able to monitor adherence to these policies.

***Management response.*** *Agreed. The information management (IM) policy will be rewritten to clarify the new accountability roles and responsibilities. The IM team just completed an organizational review resulting in new job descriptions.*

1. **Conclusion**

**37.** Based on our observations and findings, we concluded that the Office of the Auditor General is not effectively monitoring the use and implementation of PROxI, its electronic document and records management system for non-audit records. As a result, the Office cannot assess the extent to which it is meeting its document management requirements. We concluded that there are gaps in the Office’s information management policy suite and in PROxI use, in addition to the lack of monitoring and lack of reporting to support senior management’s oversight.

1. **A propos de L’Evaluation**

Practice Review and Internal Audit (PRIA) provides the Auditor General with independent and objective information, advice, as well as consulting and assurance services, to add value and improve audit practices and Office operations, through learning and continuous improvement.

As part of our internal audit process, we obtained management’s confirmation that the findings reported in this document are factually based.

**Objectives**

The objective of the internal audit was to determine whether the Office of the Auditor General is meeting its document management requirements through use and implementation of its information management system.

**Scope**

We focused our internal audit on areas of the Office responsible for the development, implementation, and maintenance of the PROxI system, in particular the information management (IM) and the information technology (IT) areas that deal with information management.

**Application Features Evaluation Criteria**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **POSSIBLE VALUES** | **FS**: Fully supported | **PE**: Paid enhancement | **NS**: Not supported | **>50%** = mandatory |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **APPLICATION FEATURE** | **SYSTEM** | **Delivery Method** | **Enhanced cost** | **Importance level** |
| Does the application enable a real time dashboard view? |  |  |  |  |
| Does the application enable dashboard customization? |  |  |  |  |
| Profile |  |  |  |  |
| Messages |  |  |  |  |
| Subscription |  |  |  |  |
| Workflows |  |  |  |  |
| Mailed documents |  |  |  |  |
| Documents |  |  |  |  |
| * Check-in/check-out |  |  |  |  |
| * Downloads |  |  |  |  |
| * Favorites |  |  |  |  |
| * Recently used |  |  |  |  |
| * Deleted |  |  |  |  |

### Audit Capabilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AUDIT CAPABILITY** | **SYSTEM** | **Delivery Method** | **Enhanced cost** | **Importance level** |
| Does the application provide the ability to identify the person making the change? |  |  |  |  |
| Does the application provide the ability to identify the date and time the change was made? |  |  |  |  |
| Does the application provide the ability to identify the document/record involved in the activity? |  |  |  |  |
| Does the application provide the identity of the action being performed? |  |  |  |  |
| **Data Audit Security**: Does the application have a native ability to track audit details about the following events; |  |  |  |  |
| * Clear (when the view list is cleared) |  |  |  |  |
| * Select (when a document is selected in a list) |  |  |  |  |
| * Favorites |  |  |  |  |
| * View (when the current view list is viewed) |  |  |  |  |
| * Pages (when a page of a document is edited) |  |  |  |  |

**Workflow Process**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **WORKFLOW PROCESSING** | **SYSTEM** | **Delivery Method** | **Enhanced cost** | **Importance level** |
| Can a specific workflow definition be exported to an XM-file? |  |  |  |  |
| Are the processed data maintained internally as XML |  |  |  |  |
| Does the application provide the ability to identify the document/record involved in the activity? |  |  |  |  |
| **Document standards**: Which of the following standards are supported by the application? |  |  |  |  |
| * Hypertext Markup language (HTML) |  |  |  |  |
| * Document type definition (DTD) |  |  |  |  |
| * Extensible markup language (XML) |  |  |  |  |
| * Extensible stylesheet language transformation (XSLT) |  |  |  |  |
| * XML Schemas |  |  |  |  |
| * JAVA Server Pages (JSP) |  |  |  |  |
| * Web service definition language (WSDL) |  |  |  |  |
| **Which Business Process Management Standards (BPM)**: are supported |  |  |  |  |
| * WARIA |  |  |  |  |
| * WfMC |  |  |  |  |
| * BPMi |  |  |  |  |
| * WfXML |  |  |  |  |
| * UDDI |  |  |  |  |
| is a rules editor available or the rules engine extendable? |  |  |  |  |

**Extended Features**

Archiving

**Application Performance**

Latency

Test environment

Test performance

**Application Maintainability**

Development environment setup performance

Change implementation performance

Release performance

**Project Governance**

Project resource availability

Incidence management

Management support in change implementation

**ROI Return On Investment**

Training plan,

Training documentation

**Note Gobal des évaluations**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **EVALUATION GLOBAL** | **REPONSE** | **Time to Deliver** | **Enhanced cost** | **Appreciation** |
| **SUPPORTABILITY INDEX** |  |  |  |  |
| **MAINTENABILITY INDEX** |  |  |  |  |
| **MANDATORY ENHANCEMENT COSTS** |  |  |  |  |
| **PERFORMANCE OF FULLY SUPPORTED STADARD FEATURES** |  |  |  |  |
| **PERCENTAGE FULLY SUPORTED REQUESTED FEATURES** |  |  |  |  |
| **PERCENTAGE OF MANDATORY FEATURES TO BE ACCOMPLISHED** |  |  |  |  |
| **SYSTEM PERFORMANCE** |  |  |  |  |
| **SYSTEM USABILITY** |  |  |  |  |
| **CUSTOMER SATISFACTION** |  |  |  |  |
| **TIME NEEDED TO IMPLEMENT THE ACCEPTABLE (85%) SOLUTION** |  |  |  |  |
| **CHANGE DELIVERY CAPABILITY** |  |  |  |  |
| **PROJECT GOVERNANCE CAPABILITY** |  |  |  |  |
| **PERCENTAGE OF RETURN ON INVESTMENT(ROI)** |  |  |  |  |
| **OVERALL SCORE** |  |  |  |  |

1. **Appendix**

**SYSTEMS AUDIT CHECKLIST**

**Internal and External Audit**

(1) Internal audit program and/or policy

(2) Information relative to the qualifications and experience of the bank.s internal auditor

(3) Copies of internal IS audit reports for the past two years

(4) Copies of most recent IS audits performed by regulatory agencies or other outside auditors

(5) All bank responses to IS audits or regulatory examinations

(6) Minutes of audit committee minutes

**Management**

(1) Organizational chart listing individuals responsible for IS along with job

titles

(2) Any available biographical or certification data for key IS personnel

(3) Any available job descriptions

(4) Minutes of board of directors meetings for past twelve months

(5) Information about IS governance committees often called steering

committees or technology committees as well as minutes of meetings

for past twelve months

(6) Copies of all policies governing IS activity

(7) Copies of current IS insurance policies including coverage on: equipment

and facilities, media reconstruction, items in transit, employee fraud,

third-party fraud, business interruption, and errors and omissions

(8) Copies of information systems/information technology strategic plans

**Service Supplier (AYD) Management**

(1) Schedule of all applications processed in-house including the name of

software vendor and/or support vendor

(2) Schedule of all applications processed by a service bureau

(3) Any agreements with software, hardware, or network service providers

used by the bank

(4) Service providers. audited financial statements and annual reports

(5) Any third-party reviews of service providers. controls over information

technology and related processes such as SAS 70 reports

(6) Any information about the disaster recovery program and the testing of

same for key service providers

(7) Any evidence documenting due diligence with respect to management of

vendors such as the way primary outsourced vendor invoices are

reviewed for accuracy

(8) Information about the bank.s involvement in user groups

(9) Procedures for implementing core software vendor release updates

**Development Process**

(1) Procedures, policies or standards governing the developpeent of new RFC (request for changes) of technology

(2) Information about any major incidence or change

- (a) recently completed,

- (b) currently underway, or

- (c) planned for the future

(3) Information about the development and use of database maintenance

Carried out by the bank

(5) Information about the management, organization, and storage of

software licenses for software being utilized by the enterprise

**Operations**

(1) Schedule of all significant computer equipment including manufacturer,

model, operating system if applicable, and as many other identifying

characteristics as possible

(2) Operator check lists, user instructions, run books, or other

documentation of this type

(3) Procedures designed to facilitate separation of operational duties

(4) Procedures relative to master file changes such as changes of address,

due dates, etc.

(5) Procedures or policies relative to the handling of negotiable items

(6) Samples of any manual logs maintained to track IS-related events or

Problems

**Information Security**

(1) Any information relative to a formal information security program

(2) Any information relative to a formal risk assessment program

(3) Any external reports, studies, or assessments of risks relative to

information security

(4) Diagrams or schematics of local and wide area networks

(5) Information about network access controls including firewalls, application

access controls, remote access controls, etc.

(6) Information relative to the management, configuration, and monitoring

of the network firewalls

(7) Lists and samples of any firewall-generated reports, logs or alerts

(8) Information relative to intrusion protection

(9) Authentication controls including password standards for the network as

well as the host processor

(10) Lists and samples of any system-generated reports or logs or any

special software used to automatically monitor and report system

activity relative to either the network, or any ancillary systems

(11) Vulnerability assessments and/or penetration tests

(12) Information relative to security education of employees

(13) Nondisclosure agreements with vendors

(14) Any information about the use of virus protection software

(15) Information about physical security including locks, fire extinguishers,

sprinklers, etc.

(16) Employee handbooks, standards, or policies

(17) Information about any disclosures or contracts signed by employees

relative to information systems

**Business Continuity**

(1) Business continuity plan

(2) Emergency preparedness plans

(3) Inventory of offsite storage facilities

(4) Contracts with business continuity providers

(5) Schedule of equipment and other resources at the designated alternate

processing site

(6) Reciprocal agreements with other banks or businesses

(7) Reports of recent business continuity tests

(8) Documentation of vendor assurances relative to business continuity

(9) Procedures, and/or schedules relative to the media backup of all data on

all servers including standalone PCs, networked PCs, core processing

system, and all ancillary systems

**Electronic Banking**

(1) Information regarding documented internet banking, telephone banking, and other

electronic banking activities engaged in by the bank

(2) Procedures relative to customer user profiles and passwords

(3) Daily procedures carried out by employees relative to electronic banking

(4) Copies of policies and procedures governing electronic banking activities

(5) Copies of contracts with electronic banking vendors

(6) Network schematic to identify the location of major e-banking components

(7) Information relative to the number of customers who use the various

electronic banking applications

(8) Information relative to risk assessment of electronic banking activities

(9) Information relative to the design and maintenance of the bank’s website

(10) Information relative to the flow of information between the bank’s

electronic banking applications and the bank’s core processing system