

Chief Review Services

**FMAS APPLICATION SECURITY
AND BUSINESS PROCESS CONTROLS**

July 2000

7050-7-18 (CRS)



TABLE OF CONTENTS

PART 1 - RESULTS IN BRIEF 1

PART 2 - INTRODUCTION 4

 General 4

 Scope 4

 Methodology 5

 Document Organization 6

PART 3 - APPLICATION SECURITY CONTROLS 7

 General Assessment 7

 Access Authorizations 7

 BASIS Team Administration 10

 Summary 13

PART 4 - BUSINESS PROCESS CONTROLS 14

 General Assessment 14

 Accounts Payables and Workflow 14

 Vendor Master Record Maintenance 15

 Invoices and Credit Notes 16

 Use of Substitutes and Bulk Approvals 17

 Accounts Receivable 18

 Customer Master Record Maintenance 19

 Material Master Maintenance 19

 Cash Collection 20

 Recording of Invoices/Credit Memos 21

 Customer Account Balances Monitoring and Management 22

 Summary 22

PART 5 - SUMMARY AND CONCLUSIONS 24

PART 1 - RESULTS IN BRIEF

1. This report presents the results of the Chief Review Services (CRS) review of the controls over the Financial and Managerial Accounting System (FMAS) application security and the high-risk areas of the associated business processes (Accounts Payable, Accounts Receivable, etc.). The review was conducted at the request of Director of Managerial Accounting Control (DMAC) to support the upgrade of the FMAS SAP/R3 software to a new version (ISPS6).
2. This report is one of a series of CRS reviews that have assessed local and departmental management practices. The financial framework of the Department, in particular, has undergone a tremendous amount of change, including the redefinition of the comptroller role and the implementation of the FMAS application. As reported in the CRS review of operating budgets, the changes have eliminated many of the traditional financial controls and placed more emphasis on the roles and responsibilities of the Responsibility Centre Managers (RCM).
3. This review complements other CRS reviews by addressing the interplay and interdependence of the FMAS application security controls and controls in the business process areas (See Chart 1 page 3 -FMAS Control Environment). As part of this review, CRS also developed a control matrix, provided to DMAC 4 under separate cover, that can be used to assess future modifications and enhancements to the FMAS application system.
4. Application Security. The review of the FMAS security focused on the controls over the assignment and maintenance of users and the FMAS programmers. Our overall assessment is that there are no serious application security exposures in the FMAS system. The FMAS security administration procedures and the user authorization design are adequate. However, several issues, primarily involving conflicting user profiles, were evident. We understand that the planned implementation of an enhancement to the FMAS authorizations and profiles program will address the recommendations in this area. In addition, many of the recommendations concerning the monitoring and control of the FMAS BASIS and Project teams have already been implemented.
5. Business Processes. The business process control portion of the review assessed the controls over the high-risk business transactions processed through the FMAS application. Although the review found that the business processes controls in FMAS were generally adequate to address the main areas of risk, weaknesses were observed in the associated local financial controls. This finding is consistent with previous CRS reviews in this area and supports the requirements for improved financial management and control at the local level.
6. Our recommendations centre on two areas: the control and monitoring of FMAS users and programmers, and the strengthening of non-FMAS financial controls at the Regional Departmental Accounting Office (RDAO) and local levels. These are two significant control areas that contribute to the financial control framework, ensuring the appropriate recording of expenditures and the timely recognition of revenues. Director Financial Policies and Procedures (DFPP) and DMAC are implementing changes in these areas to address the issues raised.

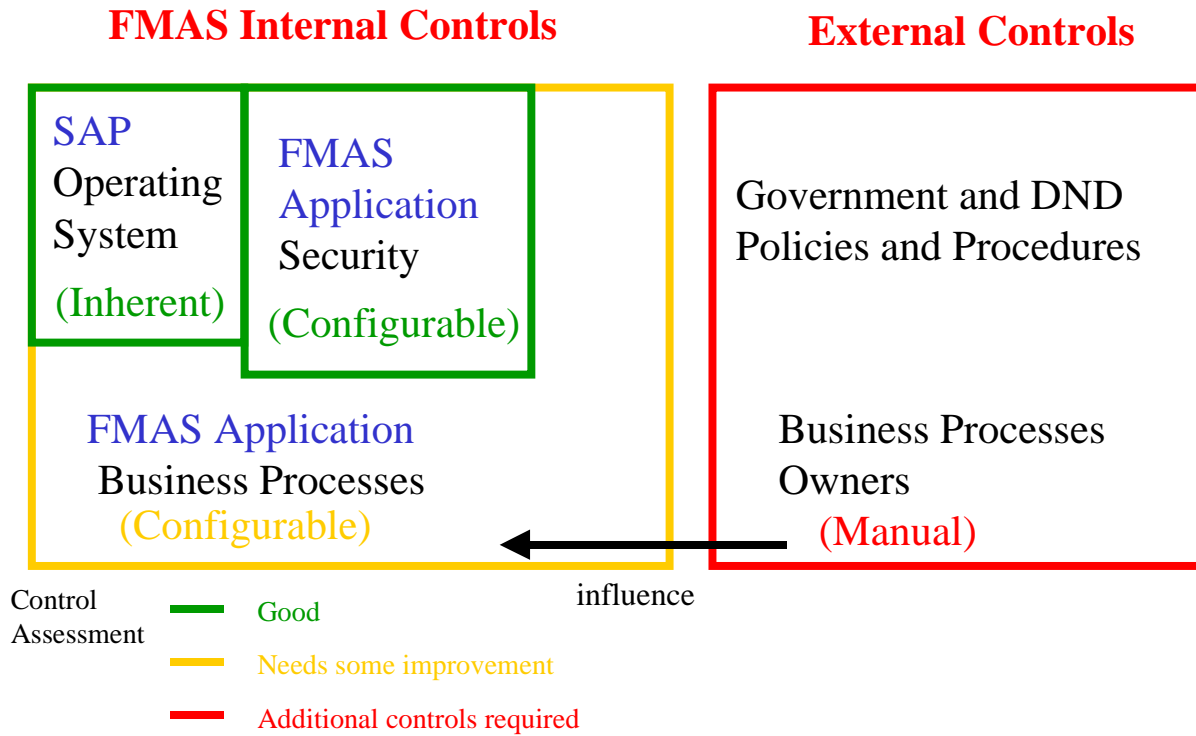
7. While some of the recommendations require modifications to the FMAS application, others only affect the manual financial controls within the non-FMAS business process. The proposed changes will:

- provide tighter control over the Vendor and Customer tables to address weaknesses in the controls over duplicate payments and uncollected revenue;
- provide an enhanced capability to check for possible duplicate payments;
- contribute to the further strengthening of the review of transactions by the Section 33 authority;
- provide direction to Comptrollers with respect to the requirements of the Local Access Control Officers (LACOs) to ensure that users are monitored and controlled; and
- improve the ability of the Central Departmental Accounting Officer (CDAO) to monitor outstanding customer balances and to match revenues to invoices.

In addition, a key financial instruction, addressing the area of expenditure management, is being prepared by DFPP in the form of a DAOD. This instruction will clearly state the financial responsibilities, under the Financial Administration Act (FAA), of the RDAO manager/comptroller, the Section 33 and 34 authority holders, and RCMs.

8. The implementation of the recommendations contained in this report will help the Department when it proceeds with the upgrade to the latest version of the SAP software. Further, it will improve the FMAS application security and business process control framework protecting the Department of National Defence (DND) financial resources. The improved control over user authorizations, and the promulgation of direction concerning expenditure management, will address specific control issues raised by our review both at the NDHQ and local levels. However, the recommendations should not be considered in isolation. Recommendations contained in the CRS reviews of Operating Budgets, Local Procurement and Supply, and the Chart of Accounts are related and relevant to the overall management framework.

FMAS Control Environment



PART 2 - INTRODUCTION

GENERAL

9. At the request of DMAC, CRS undertook an application security control review, and business process control assessment, of the SAP-based FMAS at DND. This review was conducted under the direction CRS utilizing consultants from PricewaterhouseCoopers (PwC).

10. The implementation of the SAP is often accompanied by significant organizational, process and technological changes. These changes, along with the highly integrated nature of the SAP system, present a number of data integrity risks that needs to be managed and mitigated through new approaches to security and process controls.

11. Application Security Controls. The objective of the application security controls part of the review was to assess the adequacy of the access controls to the FMAS system. The SAP application security controls, including the SAP user authorizations, are central to the integrity of the access controls and segregation of duties in FMAS. The SAP security administration impacts all aspects of the application - from its management activities to the processing of the business transactions. Consequently, the design, maintenance and management of the security controls is critical to ensuring the protection of data in the SAP environment.

12. Business Process Controls. The objective of the business process control part of the review was to assess the FMAS controls over the business transactions processed through the application. The business process controls impact upon the confidentiality, integrity, accuracy, completeness and availability of data. These controls should ensure that financial and operational data integrity risks are identified and properly managed.

SCOPE

13. FMAS has been in production in DND since April 1, 1998 with the following modules: Accounts Payable (AP), Accounts Receivable (AR), Workflow (WF) for payment processing, Funds Management (FM), Project System (PS), Purchasing and Materials Management (MM), and Sales and Distribution (SD).

14. The scope of the review focused on:

- the application security controls in the FMAS production system (SAP client); and
- the business process controls in FMAS for high-risk transactions in Finance-Controlling (Accounts Payable and Accounts Receivable), Workflow, Funds Management, Project Systems, Materials Management and Sales and Distribution modules.

15. CRS has recently performed other reviews that have commented on the adequacy of management controls. Therefore, the scope of the review was limited to the FMAS system controls and did not include testing of manual controls. In addition, the security and controls surrounding the technical infrastructure, conversions, and interfaces with other application systems at DND and other government entities were not part of this review.

METHODOLOGY

16. The PwC Security and Controls Methodology was used to perform this review and, where needed, was tailored to the SAP environment at DND. The key elements of the methodology are described below.

17. Application Security Controls. The review included a review of the user authorizations and the authorities granted to members of the FMAS BASIS and Project teams. It also included interviews with key members of the FMAS BASIS and Security teams, and the examination of the security administration policies and procedures and the BASIS administration and change management controls. The review made use of the PwC software SAPAT (SAP Audit Tool¹) to review the application security controls. SAPAT facilitated the analysis and identification of potential segregation of incompatible duties, or unusual access rights, concerns.

18. Business Process Controls. The review examined the current business processes and identified best practices. It included:

- Meeting with DND personnel to review the business processes and identify the associated risks. Representatives included key staff in the Financial and Managerial Accounting Project (FMAP), DFPP, CDAO, and the Materiel Group.
- Rating of the risks associated with SAP transactions as high, medium or low in conjunction with representatives from FMAP.
- Defining the control objectives related to the business process identified as having a high-risk.
- Documenting the existing controls in FMAS for the high-risk business processes. The current controls were one of three types: SAP inherent, SAP configurable or manual.
- Assessing the controls, using the PwC database of SAP business process control objectives and procedures; and, where the existing controls did not meet the control objectives, recommending additional controls based on best practices.

¹ PwC proprietary software

DOCUMENT ORGANIZATION

19. The remainder of this report concentrates on the macro-level issues, providing an overall assessment of security and controls surrounding FMAS, key findings identified during the review and recommendations for improvement. We have provided DMAC with the detailed review results, under separate cover, including the following:

- Record of Audit Observations. The detailed record of all observations, the analysis of these observations in terms of current controls in place if applicable, risk implication to DND, best practices (controls) to be considered for DND, and management responses to the review recommendations.
- List of High Risk Transactions. A list of high-risk SAP transactions identified by the FMAS and CRS representatives.
- Control Matrices. A detailed listing of the control objectives for each business process, including the results of the review and recommendations for improvements/additional controls.

PART 3 - APPLICATION SECURITY CONTROLS

GENERAL ASSESSMENT

20. A review of the security administration policies and procedures controls for BASIS administration and change management procedures determined that there are no serious security exposures. A summary of the identified strengths is presented below:

- The FMAS security administration procedures and the design of user authorization controls are well documented.
- The user authorization design strategy has been carefully considered and implemented. The design approach greatly facilitates the on-going authorization maintenance and trouble-shooting functions.
- A periodic query in SAP is run by the Functional Application System Manager (FASM) Authorization Officer in DMAC 4 to ensure that user access to multiple functions are appropriate and not conflicting. A checklist of conflicting profiles is maintained by the FASM Authorization Officer and used to perform this procedure.
- The Department's security administration documentation on the maintenance of user authorizations is clearly written and available to all DND personnel on the FMAS web page.
- Change management controls procedures are documented including procedures required for change requests, OSS notes application, and expected service levels.

Notwithstanding the above general assessment, the controls over *access authorizations* and *BASIS team administration* require ongoing attention to ensure a continued secure system environment in FMAS.

ACCESS AUTHORIZATIONS

21. Although the central control of user authorizations by the FASM Authorization Officer is generally well managed and monitored, there are significant access risks at the local level. During the review, staff expressed concern that the LACOs in the individual units often lacked sufficient training and/or financial expertise to properly perform their duties. In addition, there were concerns that the LACOs were not adequately supervised or monitored. These concerns have also been noted in previous CRS reviews. Properly trained LACOs are critical to ensure that user authorization rights are in accordance with their organizational roles and responsibilities.

22. The security administration function is decentralized with the FSAM Authorization Officer, in DMAC 4 at National Defence Headquarters (NDHQ), providing support and training to the LACO. The control framework at the local level relies on the local comptroller and the LACO. The comptroller, a senior financial officer at the unit level, plays a critical role in FMAS system security. According to FMAS Web site, the comptroller's responsibilities include:

- ensuring that all applicants for FMAS meet the necessary prerequisites for profiles (e.g., ensures applicants have the appropriate Section 33 and 34 authority under the Financial Administration Act (FAA));
- ensuring adequate personnel are appointed to LACO positions;
- liaising with the LACO to ensure appropriate user access rights are granted and user audits are performed;
- notifying the FASM Authorization Officer when problems related to access rights arise; and
- ensuring proper handover when LACO turnover occurs.

23. The LACO, the first point of contact for the user, has the following roles and responsibilities:

- establishing and monitoring user access to the FMAS system for users in their identified area of responsibility;
- assigning profiles to match the user's business role and responsibility; and
- maintaining workflow hierarchy to ensure the proper flow of transactions within the system.

24. The poor controls at the local level have resulted in various user access concerns, including:

- the creation of user ids with conflicting authorizations (Section 33 and Section 34 profiles) - three users identified;
- the existence of active user ids for persons who are not longer in the Department or have moved to different locations and jobs;
- the high number of users with upload capabilities to FMAS - 1,022 users identified;

- users with more than one user id without a valid business reason; and
- LACOs with access to the system through other user ids - three users identified.

Note: Further details can be found in the Record of Audit Observations, provided to DMAC 4 under separate cover.

Recommendations

25. The following recommendations are aimed at ensuring that adequate controls over user authorizations are established at the local level:

- (R1) A person under the direct supervision of the Regional Department Accounting Office (RDAO) Manager/Comptroller should occupy the LACO position at each location.
- (R2) The RDAO Manager/Comptroller should be responsible for recommending and endorsing the granting of all Section 33 authorizations.
- (R3) The RDAO Manager/Comptroller should ensure that new users, with limited experience and knowledge of FMAS; users with no formal FMAS training; and users that perform only occasional entry; are designated as high-risk when their user ids are created.
- (R4) LACOs should not be permitted to have any other FMAS user id.

At the central level controls over user authorizations include:

- (R5) The FMAS Authorization Officer should regularly review user ids for incompatible functions and monitor the LACO activities. The FMAS Authorization Officer should also review the Security Administration documentation on the Department Wide Area Network (DWAN) to ensure that it is still up-to-date and relevant.
- (R6) The FMAS Authorization Officer should revise the FMAS program to identify high-risk transactions for Section 33 review.
- (R7) A program should be written to automatically lock users who have not logged on in 90 days. Notification should still be sent through the chain of command to the users. After an additional 30 days of inactivity, these users should be removed from the system.
- (R8) All users should be assigned to the appropriate user group to ensure a designated user administrator performs proper maintenance.
- (R9) The BASIS and Project teams should be split into two separate user groups.

Management Response

- (M1) DFPP will develop and promulgate instructions/policies informing the RDAO Manager/Comptroller of the requirement to supervise the LACO.
- (M2) Direction will be provided to the RDAO Manager/Comptroller concerning the granting of Section 33 authority.
- (M3) Direction will be provided to the RDAO Manager/Comptroller and LACO concerning the creation of new users, the identification of high-risk users.
- (M4) Direction will be provided to LACOs concerning the restrictions on having more than one user id.
- (M5) An enhancement to the Authorizations and Profiles program in FMAS will address many of the conflicting user profile issues observed upon by this review. In addition, the FMAS Authorization Officer will continue to run scheduled jobs to identify invalid profile combinations and to monitor the situation. However, it should be noted that there are instances where multiple accounts are needed to segregate roles in the system, as the combination of profiles can result in restricted capabilities. For example, separate accounts are needed for Receiver General profiles, Director Budget profiles, LAN Administrator profiles, Accounts Receivable profiles and Accounts Payable profiles.
- (M6) DMAC 4 / FMAP Team Leader will investigate the problem with the sampling program and correct it if possible.
- (M7) A new FMAS program has been written and moved into production to allow LACOs to report on users within their user group that have not logged in for a specified period of time. As a result, the LACOs will be able to easily investigate and remove accounts that are not needed. In addition, there are two new reports in production that will be run by the BASIS team. The first will lock user-ids that have not been used for a period of time, and the second will delete these accounts.
- (M8) All users have been set up under a user group. Jobs are being run to find users without a user group - these are considered errors and will be corrected when discovered.
- (M9) The BASIS team members are now set up under the BASIS user group. The rest of DMAC 4 / FMAP team are set up under the Project group.

BASIS TEAM ADMINISTRATION

26. In general, the authorities granted to members of the BASIS and FMAS Project Teams could be tightened. The initial implementation of FMAS demanded flexible and dynamic BASIS and Project teams; therefore, the controls over access rights were fairly liberal. As a result, team

members with authorization to system administration objects were given access to sensitive system functions. However, now that the initial implementation has been completed, this level of access can result in unauthorized access or alteration of FMAS data. In addition, there are cases where the authority levels provide the team members with unrestricted access to the system. For example:

- There are 14 users with a profile (SAP_ALL) that gives them unlimited access to the system. This authority allows them to perform virtually all functions in the production system, including security, financial, systems operation and management functions.
- There are 14 users with a profile (SAP_NEW) that allows them access to previously unprotected transactions and to retain their prior access rights, (even if the transactions have been secured in the new release), until the security administration can assign the appropriate access.

Additional concerns were raised over the control of authorization allowing BASIS Team members to access ABAP programs, 17 users with authorization to table maintenance transactions (such as SM31), and 26 users with the object permitting the scheduling of jobs (S_BTCH_NAM). Finally, 8,765 users had access to the system administration function RSET.

Recommendations

- (R10) The FASM Security Officer should review and rationalize the BASIS team's requirements with a view to restricting or controlling access to key SAP profiles.
- (R11) Access to the 'Systems Administration Functions' authorization object should be secured and restricted to authorized personnel in the BASIS team. User access to the system administration object RSET should be restricted before this archiving function is implemented.
- (R12) All ABAP program creation, modification, and deletion should follow the FMAS change management control process for transport to the production system. ABAP programs should be secured by assigning them to authorization groups that are restricted to authorized users.
- (R13) Tables are normally updated as a result of SAP transactions, but can also be maintained in the specific table maintenance transactions. The requirements for table changes in production should be documented and access should be restricted to authorized users; access to tables maintenance in production should be secured through assignment of authorization groups to tables; and access to these groups should only be given only to authorized users.

- (R14) The authorization object is used to specify a user name other than the current user when scheduling a background job. Users with this authorization object can execute a batch job that will use the authorization profile of any user id named in the batch job. Therefore, access to this facility should be granted only to the system administrator and the interface manager. In addition, authorization to write ABAP programs (S_DEVELOP), to the object allowing the user to develop programs and customize the system (S_TRANSPRT), and to ABAP Workbench components should be restricted.

Management Response

- (M10) The DMAC 4/FMAP Team Leader has reviewed the risks associated with the current control over the profiles SAP_ALL and SAP_NEW and determined that further restriction of these profiles would not be cost beneficial. In SAP other system exposures would still exist. In addition, restricting access to these profiles would likely require the hiring and training of more personnel to establish a 'one job - one person model'. This would partially negate the current benefits of cross training which allows BASIS staff to be very flexible in the event of leave or illness or scheduled training. Finally, a large effort would be required to create custom profiles in the system for BASIS, and currently the BASIS resources are busy with Y2K and upgrade priorities.
- (M11) The profiles ZD:RIO:DMC and ZD:UCO:MGR give RSET in authorization object S_ADMI_FCD. Currently, SAP archiving transactions are not available and so this poses no problem. However, the granting of RSET authorization will be reviewed if SAP archiving capability is implemented.
- (M12) Access to the ABAP programs has been secured and all program creations, modifications and deletions follow the change management control process.
- (M13) FMAS Security Officer has removed SCC4 authority from the two users in the HELP DESK group; the SCC4 review has been completed and all unnecessary access has been removed; and all update (under S_TABU_DIS) is restricted to an authorization group.
- (M14) The DMAC 4/FMAP Team Leader has determined that this does not constitute an unreasonable level of risk since any user with authority to the S_BTCH_NAM authorization already has the authority to perform the same task using the SAP_ALL or SAP_NEW profile. Production is marked not modifiable and cannot be changed to modifiable without the authority of DMAC 4/FMAP Team Leader. As a result, no one can write/change ABAP programs or create dictionary objects. Hence, there is no significant risk with the current assignment of S_DEVELOP, S_TRANSPRT or SE09/SE10 authorizations.

SUMMARY

27. Generally, the application controls were deemed to be adequate given the associated risks. DMAC 4 has reviewed the review observations and recommendations to assess the level of risk. DMAC 4 has implemented, or plans to implement, the suggested recommendations in areas where the risks warranted an increased level of control. Action taken by management includes:

- modification to existing user profiles and monitoring of user access authorizations;
- changes to, and monitoring of, the authorities granted to the BASIS and Project team members;
- access to system objects granting authority to modify the application have been reviewed and tightened where appropriate; and
- upgrade/enhancement to the Authorization and Profile program in FMAS to improve the monitoring of user access authorities.

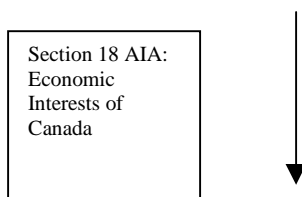
In addition, DFPP is developing financial instructions/policies to ensure the RDAO Manager/Comptrollers provide adequate monitoring and control over the persons fulfilling the LACO role. These activities will strengthen the application security controls.

PART 4 - BUSINESS PROCESS CONTROLS

GENERAL ASSESSMENT

28. While the controls in the business processes for Funds Management, FMAS Operations, Master Data Maintenance, and Reconciliation with Public Works and Government Services Canada (PWGSC) were deemed to be adequate to address the main areas of risk, certain manual or procedural controls supporting the FMAS application in the other business processes require strengthening. Many of these control weaknesses have been identified in other reviews performed by CRS including the reviews of Operating Budgets, Local Procurement and Supply, and the Chart of Accounts.

29.



ACCOUNTS PAYABLES AND WORKFLOW

30. The SAP system is used in the DND/CF as the primary financial accounting system, and is referred to as the Financial Managerial Accounting System (FMAS). The main function of the accounts payable module is to serve as a vendor invoice processing system. However, a limited number of purchase orders are entered and processed using the FMAS.

31. Invoices are manually approved for payment by the FAA Section 34 authority and entered into FMAS. The approved payable transactions released for payment are electronically sent to PWGSC, which in turn issues cheques to the vendors. The confirmation of payment is sent electronically from PWGSC to DND. These electronic transactions are processed in FMAS as cheque numbers for requisition of payments.

32. The business functions risk assessment portion of this review identified three processes in Accounts Payable module in FMAS as having a higher risk: *Vendor Master Record maintenance, Invoice and Credit Note processing, and the Use of Substitutions and Bulk Approvals.*

Vendor Master Record Maintenance

33. The control over the creation of vendor master records is not adequate. Central control is maintained over certain vendor types, however, all users with the ability to enter invoices (Section 34) are permitted to create vendor master records for non-centrally controlled vendor types. This allows users to inappropriately enter duplicate vendors or invalid vendor records in the vendor master record table.

Section 18 AIA:
Economic
Interests of
Canada



Recommendations

- (R15) Creation of new vendors should be restricted as follows:
- Other Government Departments (ZOGD), Financial and Banking Institutions (VBNK) and DBA onetime vendor (CPDL) should be restricted to FMAS team.
 - Vendors with annual sales greater than \$30,000 (VNDR) and Occasional Vendors (NONS) should be restricted to CDAO and RDAO personnel based upon a request from a Section 34 authority.
- (R16) Only RDAO personnel should be permitted to make changes to VNDR and NONS vendor master records.
- (R17) Procedures outlining the proper use of the miscellaneous vendor record (ONETIME) should be developed and distributed to all Section 34 authorities.
- (R18) Naming Standards for Vendors and standards for entry of invoice information should be developed and distributed to Section 34 authorities.

Management Response

34. Centrally managing the vendor master records at the RDAO level would greatly improve the current situation. However, this shift in responsibility could strain the Comptroller's scarce resources. The change to the vendor table maintenance should be as follows:

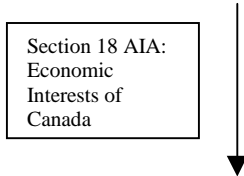
- (M15) Vendor types ZOGD, VBANK and CPDL: Maintenance will remain the exclusive responsibility of the FMAS team as it is being currently done. Vendor types VNDR and NONS: An ADM(Fin CS) directive will be sent instructing the RDAOs to maintain (create and modify) these vendors.
- (M16) The FMAS application will be modified to prevent users from creating new vendors.

(M17) ONETIME vendors: once the vendor master records are maintained centrally, the ONETIME vendor facility will be removed as a valid selection. This will prevent users from using the ONETIME vendor facility to bypass the centralized vendor controls.

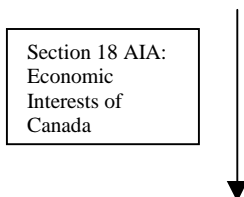
(M18) DFPP and DMAC 4 will clarify the directives on how to input vendors in FMAS to further ensure the standardization of the vendor records.

Invoices and Credit Notes

35.



36.



Recommendations

(R19) Section 33 authorities should be directed to perform a detailed review of all transactions coded to ONETIME vendor record.

(R20) The FMAS program to identify high-risk transactions should be adjusted to ensure that transactions that have high dollar amounts, or are processed by high-risk users or are coded to high-risk vendors, are selected.

(R21) Section 33 authorities should be reminded of the requirement to review all high-risk transactions and perform a detailed after-the-fact review of a statistical sample of transactions.

(R22) Cost Centre managers should be reminded of their responsibility to verify expenses against budget and commitments on a regular basis (minimum monthly). Direction should be provided to Cost Centre managers on how to use FMAS reports to assist in reviewing expenses.

(R23) FMAS control over duplicate payments should be modified to only include Vendor Number and Invoice Number.


- (R24) A report on possible duplicates, by RDAO, should be developed to support the analysis, by RDAO personnel, of possible duplicate payments.
- (R25) Credit notes should be properly linked to original invoices and processed in a timely manner with an appropriate audit trail.

Management Response

- (M19) The elimination of the ONETIME vendor facility will remove the requirement for Section 33 authorities to perform a detailed review of all transactions coded to ONETIME vendors.
- (M20) DMAC 4 / FMAP Team Leader will investigate the problem with the sampling program and correct it if possible.
- (M21) DFPP is drafting DAOD's on Expenditure Management (DAOD 1005 series), which will emphasize the financial responsibilities of the FAA Section 34 and Section 33 authorities. The DAOD will clearly stipulate that persons certifying under Section 33 are required to review the payment transactions in accordance with the process listed for the particular risk level associated with the payment transaction.
- (M22) The DAOD will state the requirement for cost centre managers to reconcile their budget against their expenditure using the Planned Variance Report (PVR) report in FMAS.

(M23)

Section 18 AIA: Economic Interests of Canada




- (M24) A standard report on possible duplicates, by Cost Centre, is available on the system and a report on possible duplicates, by RDAO, will be developed in the next fiscal year. These reports will facilitate monitoring for duplicates by Section 33 authorities.
- (M25) Credit notes should be linked to original invoices and processed in a timely manner.

Use of Substitutes and Bulk Approvals

37.

Section 18 AIA: Economic Interests of Canada



38.

Section 18 AIA:
Economic
Interests of
Canada



Recommendations

- (R26) Comptroller should be responsible for ensuring that only properly authorized individuals are identified as Section 33 substitutes.
- (R27) Section 33 authorities should be instructed on the proper use of the bulk approval option.

Management Response

- (M26) Agree - the Comptroller should ensure that only authorized individuals are identified as Section 33 substitutes.
- (M27) DFPP will publish Bulk Approval and Sampling procedures in the Expenditure Management DAOD.

ACCOUNTS RECEIVABLE

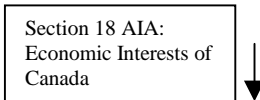
39. The Accounts Receivable module in FMAS is used as an invoicing and cash collection system. Sales of both products and services are invoiced through the FMAS system. However, distribution and inventory management functions are not performed through FMAS. Sales activities are decentralized and occur at many DND locations. Most of the invoicing that is performed using the FMAS system is centralized at the CDAO. However, some invoicing functions may be performed outside the FMAS system. The cash collection activity is also centralized at the CDAO, although certain DND locations use a local Receiver General Deposit Facility (RGDF).

40. The revenue earned can be treated a governmental, DND corporate or DND local revenue. The location for the retention of revenue is defined by the Retention of Local Revenue Policy. The revenue is based on the material sold and is coded in the material master table in FMAS.

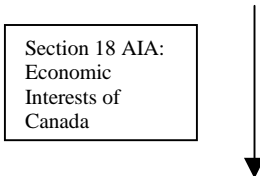
41. The business functions risk assessment portion of this review identified the following five processes in Accounts Receivable as having a higher risk: *Customer Master Record, Material Master Record, Cash Collection, Recording of Invoices/Credit Memos, and Customer Account Balance Monitoring and Management*. Each will be discussed in turn.

Customer Master Record Maintenance

42.



All users with the ability to create sales documents can also create the sales view for new customers.



Recommendations

- (R28) Creation of new Customers should be restricted as follows: ZOGD, ZBIL, ZONE - restricted to FMAS team; and ZFOR/ZSPE, ZINT and ZEXT restricted to RDAO personnel. The creation of ZFOR/ZSPE, ZINT and ZEXT customers should be based upon a request from the person responsible for selling goods or services and with the prior approval of the Comptroller.
- (R29) Comptrollers should perform credit checks on all customers before approving the creation of the customer record.

Management Response

- (M28) Agree - the creation of customers should be properly controlled. Therefore, ZOGD, ZBIL, ZONE customers will be restricted to the FMAS team; and ZFOR/ZSPE, ZINT and ZEXT customers will be created only with approval of the RDAO Manager/ Comptroller after adequate credit checks are conducted.
- (M29) In general, more RDAO Manager/Comptroller involvement is required in the A/R process. The evaluation of the customer should be based on past payment performance with the Department, profitability and stability of the business. DFPP will inform all Comptrollers of their requirements in this area.

Material Master Maintenance

43. The material² master data is created centrally by the development team. The material master data contains the product description, tax code, material code and material type. The review found 29 different Billing Document types, six with no billing block and two without the proper accounting information.

² corresponds to 'Materiel' in DND

Recommendation

- (R30) Remove unused billing document types and ensure all remaining billing document types have a proper billing block and accounting information.

Management Response

- (M30) The Billing Document types are SAP-delivered and unnecessary modifications to the delivered system should be avoided since this creates additional work when new releases are implemented. Currently, the use of Bill Document types is controlled via validation rules and business procedures. These should be sufficient to prevent the inappropriate use of Bill Document types.

Cash Collection

44. The majority of the cash collection activities are performed by the CDAO, but many locations in Canada have their own Receiver General Deposit Facility (RGDF) and RGDF clerks who perform cash collection activities. Locations with no RGDF, such as units outside Canada and HMC ships, have minimal receipts. Receipts are accumulated and sent to CDAO for deposit and accounting action. The CDAO matches receipts with invoices. However, if no corresponding invoice or customer is identified at the time of the cash deposit, after a period of three weeks, the revenue will be recorded as DND corporate revenue.

45. The CDAO is required to monitor actual corporate revenues to budget on a quarterly basis and should increase the frequency of the monitoring to a weekly basis for last quarter of the fiscal year. The Command and Base Comptrollers should also be monitoring actual local revenues to budget on a quarterly basis and should increase the frequency of the monitoring to a monthly basis for the last quarter of the fiscal year. The review observed that this was not the case in FY 1998/1999 or FY 1999/2000 to date.

Recommendations

- (R31) The invoice/credit memo processing should be segregated from the cash collection and account reconciliation processes at all locations.
- (R32) All receipts should be reconciled to invoices in a timely manner.

Management Response


- (M31) Agree - the cash collection should be segregated from the billing process.
- (M32) All receipts should be recorded in FMAS in a timely manner referencing the appropriate invoice.

Recording of Invoices/Credit Memos

46. Sales documents and invoices (or credit memos) are not always entered in a timely manner. In addition, we observed that some customers are manually invoiced, with a copy of the invoice is being forwarded to CDAO for entry in the system. At other times, the invoice is not recorded in the system and the receivable is only created at the time of the cash collection.

47.

Section 18 AIA:
Economic
Interests of
Canada



48. We also observed that cash collections occasionally have been ‘unintentionally’ coded to an inappropriate type of revenue (e.g., government, DND corporate or DND local). This affects the amount of funds available in the respective revenue account.

Recommendations

- (R33) Ensure that procedures for the processing of invoices/credit memos are complete, up-to-date and available to all personnel creating sales documents.
- (R34) Develop a report that identifies all sales documents that have not generated proper General Ledger (G/L) transactions.
- (R35) Reject invoices where the proper accounting view is not available or the G/L update transaction has not occurred.

Management Response

- (M33) Invoice/Credit processing procedures are available on the FMAS help site.
- (M34) The new Sales and Distribution and Accounts Receivable package will print the sales document number and the accounting document number on the printed invoice.
- (M35) The CDAO staff will be able to check for the existence of both the sales and accounting document numbers. This will make it much easier for the CDAO to ensure that the G/L accounts have been properly updated to reflect the invoice amount prior to sending out the invoice.

Customer Account Balances Monitoring and Management

49.

Section 18 AIA: Economic Interests of Canada

 ↓

50.

Section 18 AIA: Economic Interests of Canada

 ↓

Recommendations

- (R36) The outstanding customer account balances should be reconciled to reflect the outstanding receivables.
- (R37) The interest and dunning facilities and customer statements available in the system should be used to manage the outstanding customer account balances. Customers should receive dunning letters when accounts are overdue and interest should be charged on overdue accounts.

Management Response

- (M36) CDAO staff will reconcile outstanding customer balances.
- (M37) Some issues related to the delayed rollover of accounts still need to be resolved before hastening and interest charging action can be taken on all accounts.

SUMMARY

51. The recommended controls over the identified high-risk business processes will be addressed through a combination of FMAS application controls and the development and promulgation of appropriate financial instructions by DFPP. Planned management action includes:

- the enhancement of programs to check for duplicate payments and high-risk transactions;
- the restriction of user access to several FMAS tables, including the Vendor and Customer tables; and

- the development of financial instructions/policies emphasizing the roles and responsibilities of the FAA Section 34 and Section 33 authorities as well as the local RC managers and RDAO manager/comptroller.

The high-risk business processes will require careful, ongoing, monitoring as business re-engineering continues to affect the financial practices of the Department.

PART 5 - SUMMARY AND CONCLUSIONS

52. The management framework of the Department includes a complex, and dynamic, set of financial controls. Over the past few years CRS has conducted a number of reviews aimed at improving the Department's management framework and the financial controls in particular. The financial controls have two main components: the controls within the FMAS application, and the external, non-FMAS, controls. The FMAS application controls are solely within the FMAS application. They include the controls that are inherent to SAP/R3, and the application controls that are configurable. The controls that are external to the FMAS application include, but are not limited to, the controls within each of the business processes, the governmental and departmental financial policies and procedures, and the ethical environment.

53. The Department determines which of the configurable controls will be implemented, a process involving trade-offs, both in terms of cost and flexibility. The Department also has some flexibility in determining how to implement the government financial policies. The development of a proper management framework requires a co-ordinated effort of all concerned and an assessment of the risks and control costs. During the CRS review, staff from DMAC, DFPP, DAPPP and other business process areas demonstrated a clear desire to ensure that the management control framework and financial controls are appropriate for the level of risk.

54. The overall assessment of the FMAS application security controls is favourable. Generally, the FMAS application controls were deemed to be adequate given the associated risks. Security administration procedures and the user authorization design are considered adequate. Conflicting user profiles, allowing users to perform duties that should be segregated, was identified as the primary concern. In response, DMAC 4 has implemented, or plans to implement, the suggested recommendations in areas where the risks warranted an increased level of control, including enhancements to the authorization and profiles program in the FMAS application. In addition, DFPP is developing financial instructions/policies to ensure the RDAO Manager/Comptrollers provide adequate monitoring and control over the persons fulfilling the LACO role. These activities will strengthen the FMAS application security controls.

55. While the controls over the high-risk business processes in FMAS were also deemed to be adequate, the review identified some weakness in the local financial controls. The main recommendations associated with the high-risk business processes will be addressed through enhanced FMAS application controls and the development and promulgation of financial instructions by DFPP. The recommendations include developing reports to make it easier to identify potential duplicate payments and the implementation of restrictions on the creation of vendor and customer master records.

56. This review will contribute, not only to the FMAS configurable controls, but also to the business process and overall management framework. In addition, the implementation of the recommendations should prove useful to the Department when it proceeds with the upgrade of FMAS to the latest version of SAP. It is encouraging to note that many of the recommendations have already been, or are in the process of being, implemented. The major recommendation that remains to be completed is the development, and promulgation of, a revised set of financial instructions. These instructions will provide addition guidance to RC managers and RDAO managers/comptrollers concerning monitoring and control in the financial area.