National Defence / Défense nationale

ASSISTANT DEPUTY MINISTER (REVIEW SERVICES)

Reviewed by ADM(RS) in accordance with the *Access to Information Act*. Information UNCLASSIFIED.

Audit of Controls over the Reliability of Data in the Canadian Forces Taskings, Plans and Operations (CFTPO) Application



September 2016

7055-65 (ADM(RS))

Canada

Table of Contents

Acronyms and Abbreviations

ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(RS)	Assistant Deputy Minister (Review Services)
BC	Business Charter
CA	Canadian Army
CAF	Canadian Armed Forces
CFTPO	Canadian Forces Taskings, Plans and Operations
CJOC	Canadian Joint Operations Command
CRS	Chief Review Services
DND	Department of National Defence
HRMS	Human Resources Management System
IM/IT	Information Management / Information Technology
MCSC	Military Command Software Centre
OCI	Office of Collateral Interest
OPI	Office of Primary Interest
SJS	Strategic Joint Staff

Results in Brief

The Department of National Defence and the Canadian Armed Forces (DND/CAF) have a mandate to maintain the readiness of military forces and to deliver on defence operations. This involves the execution of operational deployments, training exercises and other activities required to fulfill this mandate.

The work of military taskers is critical to ensuring that mission requirements are matched with the resources needed to achieve them. The tasking process allows the DND/CAF to plan its activities in order to ensure that military requirements are appropriately resourced, providing the right mix of personnel and equipment to enable mission success.

The Canadian Forces Taskings, Plans and Operations (CFTPO) application supports the tasking process. This information system brings together departmental information on personnel and equipment capabilities and availabilities in order for military taskers to assemble the teams that will meet the specific requirements of each activity.

Overall Assessment

- The CFTPO application has input, processing and output controls to help ensure the accuracy and completeness of its data.
- Accountabilities, responsibilities and data stewardship frameworks could be improved through formal documentation.
- The accuracy and completeness of the application data could benefit from increased documentation of business rules,[1] change management processes and a user training program.

The Military Command Software Centre (MCSC) of the Canadian Army (CA) manages the system development and support for the CFTPO application. The MCSC works in collaboration with the organizations responsible for planning tasks and assigning resources, as well as with the organizations responsible for supporting the information obtained from other systems in order to deliver on a task planning capability for the DND/CAF.

Given the importance of this application in operational planning, the Assistant Deputy Minister (Review Services) (ADM(RS)) conducted an audit of the CFTPO application. This audit was undertaken to determine whether the appropriate application controls are in place to help ensure the accuracy and completeness of the CFTPO application data. The audit was conducted in accordance with the Chief Review Services (CRS)[2] Risk-based Internal Audit Plan for fiscal years 2014/15 to 2016/17.

[1] A business rule is a statement that defines or constrains some aspect of business and is intended to control or influence the behaviour of the business. For example, when developing a tasking for operations, a minimum and maximum military rank for the position must be identified.
[2] Effective May 13, 2015, CRS has been renamed ADM(RS).

Findings and Recommendations

Authority and Responsibility. A number of organizations across the CAF use the CFTPO application to conduct their tasking process. These organizations have unique requirements for the application, which poses a challenge for system development. As the differences in the tasking process used by these various organizations have not been clearly laid out, the CA is unable to undertake system development in a coordinated manner to address the individual needs of each organization.

With the exception of Chief of Military Personnel, the responsibilities and authorities regarding source data used by the CFTPO application have not been clearly defined or documented by those responsible for the safeguarding of source data. As a result, there is a risk that data may be made available through the CFTPO application for purposes other than those intended.

It is recommended that the CA, in consultation with those responsible for the tasking process and the safeguarding of source data, define and implement the authorities and responsibilities for the development and management of the CFTPO application and for the acquisition of source data.

Change Management. The personnel responsible for the tasking process, the application user community and the MCSC can request changes to the CFTPO application. While the CA receives and implements change requests from these parties, the process for initiating, developing, testing, approving and implementing the changes is informal. As a result, there is a risk that changes may not necessarily be in line with business needs.

It is recommended that the CA formalize the change management process for the CFTPO application to help ensure that changes to the application are authorized, documented and communicated, and that they function as intended and meet business needs.

Application Controls. A number of controls in the CFTPO application are in place to ensure that users enter acceptable values and navigate through the application as intended. However, there are some cases where business rules are intentionally unenforced, primarily to provide flexibility to users. The rationale for implementing, or not implementing, these business rules was not documented. As a result, it was unclear whether appropriate controls were active in the application.

The CFTPO application also has the capability to restrict user access to certain functions and data. However, there is no documentation to allow relevant tasking parties to validate whether these restrictions are in line with their needs.

It is recommended that the CA, in consultation with those responsible for the tasking process and the safeguarding of source data, document and implement all key business rules related to data input, access, processing and output controls in the CFTPO application to help ensure that information is accurate and complete, and that it meets security and privacy considerations.

Training. Online training materials and a user manual exist for the CFTPO application, but formal training is not available to all users. Due to capacity constraints, formal training is limited, and the application user manual is not up to date. Training is mainly provided on the job.

It is recommended that the CA, in consultation with those responsible for the tasking process, develop and implement a training program for the tasking process and for the CFTPO application, along with the appropriate supporting documentation.

Note: Please refer to Annex A—Management Action Plan for the management response to the ADM(RS) recommendations.

1.0 Introduction

1.1 Background

1.1.1 Tasking Process

A task is the requirement of the delivery of mission operations, training exercises and other military activities, and it is a key part of the work of the DND/CAF. Tasking is the process of temporarily allocating adequate military resources (personnel and equipment) to fulfill a departmental requirement. The tasking process involves planning for these activities to support the achievement of objectives. While there is no authoritative definition of a tasking, in general it is the process of identifying and selecting individuals who have the skill set required, along with the equipment that has the required capabilities to perform specific objectives.

In order to complete a tasking request or order, military taskers are first involved in the development of personnel and equipment requirements. Personnel specifications may include conditions such as the start and end date, minimum rank, security clearance, language proficiency, and trade specifications. Once the requirements have been established, available personnel and equipment are allocated to the tasking in line with the stated requirements, and the task is executed. Tasking decisions are important in ensuring the optimal allocation and matching of military resources to meet activity requirements.

There are three tasking categories as follows:

- **Operational** – used to identify resources for a CAF mission. For example, the Department may decide to deploy a ship as part of a mission. In order to staff this particular vessel with the required military resources, those responsible for the mission would task military members with the requisite skills and experience from other areas so that the ship is resourced to an acceptable level before deployment;

- **Incremental** – used to identify resources to perform other duties, such as cadet activities, ceremonial functions and training activities. For example, the tasking process could seek to reallocate the appropriate resources to a unit so that training exercises may be effectively carried out with the right number of participants; and

- **High readiness** – used to identify fully trained individuals for rapid deployment. A certain percentage of military members are fully trained and deployable on short notice to respond to a domestic or foreign crisis, ranging from natural disasters to terrorist attacks. These individuals are essentially pre-determined and are tasked as needed.

The Strategic Joint Staff (SJS), in conjunction with the Canadian Joint Operations Command (CJOC), is responsible for operational taskings. Other CAF components, such as the Royal Canadian Navy, the CA and the Royal Canadian Air Force conduct incremental taskings. While SJS has issued standard operating procedures for the tasking process, each organization differs slightly in the way it develops and completes a tasking. A high readiness tasking can be the responsibility of any CAF component. For example, the Royal Canadian Navy could create a

task to get a vessel ready to sail on very short notice, while CJOC could create a task to pre-identify the military members necessary to respond to a domestic or international emergency.

1.1.2 CFTPO Application

The CFTPO application supports the tasking process by helping taskers create requirements and by matching personnel and equipment to those requirements. It also supports the Chief of the Defence Staff and other commanders with information on the number, characteristics and availability of personnel and some equipment resources.

The CFTPO application aggregates information from other departmental information systems to provide an inventory of personnel and certain equipment. This information is used in the tasking process to identify resources that meet specific criteria. Specifically, the CFTPO application collects data from the following departmental information systems:

- Monitor Military Administrative Support System
- Civilian and military versions of the Human Resources Management System (HRMS)
- Military Individual Training and Education application
- Fleet Management System
- Military Employment Management System

The CFTPO application has approximately 3,000 user accounts. Nearly one-third of these users make use of the system every day.

Initially developed to support the CA tasking process, the CFTPO application has now been adopted by other CAF organizations to address their tasking needs. For the most part, the CA has funded and maintained ownership and administration of the application, which it manages through the MCSC. The CFTPO application is managed by one dedicated programmer, who performs the roles of system analyst, application developer, application administrator and database administrator. The application is also supported by additional non-dedicated personnel within the MCSC, including a backup developer, an Oracle database administrator and a helpdesk analyst. A non-dedicated trainer is also available to provide onsite training upon request.

According to Defence Administrative Order and Directive 6000-0, Assistant Deputy Minister (Information Management) (ADM(IM)) is responsible for issuing and monitoring compliance with information management and information technology (IM/IT) policies, directives, instructions and standards related to enterprise-focused applications. ADM(IM) has delegated to other organizations the authority to manage their own IM/IT assets. Since the CFTPO was originally developed solely as a CA application and not an enterprise-focused application, the Commander CA is responsible for monitoring and ensuring the CFTPO application is compliant with ADM(IM) policy requirements.

1.2 Rationale for Audit

CRS conducted a planning study of IM/IT management in 2013.[3] This study identified the reliability of data in information systems as a risk area for the Department. In 2014, CRS also assessed the Department's inventory of information systems[4] and identified the CFTPO application as a high priority application among those that were not already under review, scheduled for audit or undergoing transformation. Accordingly, the reliability of data in the CFTPO application was selected for audit coverage.

1.3 Objective

The objective of this audit was to provide assurance that appropriate application controls are in place to help ensure the accuracy and completeness of the CFTPO application data.

1.4 Scope

The audit scope included an assessment of the controls within the CFTPO application that was conducted over the January 2014 to September 2015 timeframe. The controls assessed included the following:

- **Change management controls** help ensure changes in the CFTPO application are introduced in a controlled and coordinated manner;
- **Input controls** contribute to the accuracy and completeness of information input directly into the CFTPO application;
- **Processing controls** ensure that external data does not change while in the application, and that transactions are appropriately processed; and
- **Output controls** are controls over taskings issued through the CFTPO application, along with related reporting capabilities.

1.4.1 Scope Exclusion

The audit did not include an assessment of controls for the departmental information systems that provide data to the CFTPO application.

1.5 Methodology

The audit results are based on the following:

- interviews with SJS personnel and taskers from CJOC, CA, Royal Canadian Navy, Royal Canadian Air Force and Canadian Forces Health Services group;
- interviews and process walkthroughs with the MCSC;
- review of policies, procedures and guidance documents relating to tasking, the CFTPO application, user access and software development; and

[3] CRS. IM/IT Management Planning Study, 2013.
[4] CRS. Analysis of Business Applications, 2014.

- testing of application input fields and parameters.

1.6 Audit Criteria

The audit criteria can be found at Annex B.

1.7 Statement of Conformance

The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit thus conforms to the Internal Auditing Standards for the Government of Canada as supported by the results of the quality assurance and improvement program. The opinions expressed in this report are based on conditions as they existed at the time of the audit and apply only to the entity examined.

2.0 Findings and Recommendations

2.1 Authorities and Responsibilities

Authorities and responsibilities for the development and management of the CFTPO application and its data have not been defined or implemented.

2.1.1 Requirements for the Tasking Process

The MCSC initially developed and customized the CFTPO application to support the CA tasking process. Since then, the application has evolved to support the tasking processes used by multiple DND/CAF organizations, each with its own unique requirement. Some of these differences present conflicting needs when it comes to application design, and the differing requirements have not been fully documented. Without this information, the MCSC cannot ensure each organization's specific requirements are reflected in the application.

SJS, as the organization responsible for operational taskings, has provided some guidance on the tasking process and has made efforts to work with other organizations to define minimum requirements for the tasking process. Initiatives such as the National Tasker Working Group also provide a forum for tasking organizations to discuss and improve the tasking process and to provide the MCSC with feedback regarding the CFTPO application functionality.

2.1.2 Requirements for External Source Data

In order to support the assignment of personnel and equipment to taskings, the CFTPO application collects data from a number of departmental information systems. For example, data from materiel systems, such as the Fleet Management System, provide details of certain equipment availability and driver qualifications. Human resource systems, such as HRMS and Monitor Military Administrative Support System, provide personnel details including rank, occupational trade, qualifications and security clearances. In aggregate, the CFTPO application can provide a comprehensive view of the capabilities and readiness of the CAF by identifying the training that personnel have received and the availability of military resources based on this external source data available from other information systems.

These originating information systems would typically have application controls in place to govern the access and use of the data as many of them contain information subject to privacy legislation and security considerations. However, the controls are rendered ineffective when an originating system provides data extracts to the CFTPO application. This departmental access control issue, and its related recommendations, were communicated in the October 2015 ADM(RS) Audit of HRMS Application Access Rights. As part of the management action plan resulting from that audit, departmental stakeholders will work collaboratively to address the recommendations in the report related to controlling application access rights. Specifically, stakeholders have agreed to define, document and communicate responsibilities, authorities and accountabilities related to the validation and authorization of human resources data access, as well as to validate that legitimate need for human resource information is in line with business requirements and based on the least-privilege / "need to know" principle.

During the current audit, the audit team observed that Chief of Military Personnel, who is responsible for safeguarding military HRMS data, communicated its expectations for how this data can be used and by whom. However, other providers of data extracts to the CFTPO application have not communicated similar terms and conditions for data usage. As such, the expectations of what data the CFTPO application is authorized to use, and how it should be accessed and managed, has not been documented. This issue was also raised in the HRMS Application Access Rights audit, and key stakeholders committed to develop data validation processes and to better govern and control data access. Without these documented conditions, the MCSC does not have the information needed to design and implement the controls required to meet the expectations of those responsible for ensuring source data is safeguarded and used appropriately.

2.1.3 Application Business Rules

As part of the standard development of an information system, workflows are broken down into their component procedures, steps and decision points. These workflow components are used to develop the parameters of the workflow known as business rules. As is the case with other systems, these parameters are enforced in the CFTPO application through the creation and implementation of application controls. Application controls prevent users from performing functions in the application other than those intended by the workflow. For example, the SJS tasking process requires that personnel be assigned to a task based on their military rank. Therefore, the resulting business rule is that a military rank must be included in the personnel request for any task. In the CFTPO application, an application control is created that makes populating the military rank field mandatory when defining personnel tasking requirements.

There was no formal business rule approval process implemented by those responsible for the tasking process and the safeguarding of source data. Therefore, the requirements of those responsible for the tasking processes and the safeguarding of source data that form the basis for system development of the CFTPO application have not been documented and are currently communicated to the MCSC in an informal manner. As a result, the MCSC has not formally documented the business rules for the CFTPO application. Therefore, although application controls exist in the CFTPO application, they could not be linked to documented business rules so as to ensure the application is operating in line with the requirements of the tasking process. It is important that these requirements be documented so they can be communicated to and validated by those responsible for the tasking process.

The MCSC has explained that documentation of requirements and of application business rules has been informal as a result of the systems development methodology that it has chosen to follow. Under the “agile” methodology, software development emphasizes flexibility and responsiveness to requirements and continuous improvement, rather than strict adherence to disciplined processes and comprehensive documentation. As a result, documentation for system development is recorded only as annotations in the system code.

2.1.4 Conclusion

Without the documented definition and approval of stakeholder requirements and application business rules, there is a risk that controls programmed into the CFTPO application are not in line with those intended by those responsible for the tasking process and the safeguarding of source data.

ADM(RS) Recommendation

1. The CA, in consultation with those responsible for the tasking process and the safeguarding of source data, should define and implement the authorities and responsibilities for the development and management of the CFTPO application and for the acquisition of source data.

OPI: CA

2.2 Change Management

As a result of an informal change management process, controls in the CFTPO application could not be validated to ensure that changes to the application support the continuing accuracy and completeness of information.

2.2.1 Application Change Management Process

A defined and documented change management process is an important part of the system development process. The change management process allows stakeholders to ensure that application enhancements meet business requirements, and that there are controls in place to confirm the effectiveness of implemented changes.

A well-defined change management process should also provide for the segregation of duties between the roles of business analyst, application developer, application administrator and database administrator. This is important to mitigate the risk that untested and unapproved changes to the application may be released.

Good Practices

- The MCSC and SJS staffs are in constant communication about ongoing issues and changes. Additionally, the National Tasker Working Group plays the role of a forum for users to learn about the CFTPO and provide feedback for increased application functionality.

There is no formal change management process in place for the CFTPO application. Application changes can be requested over the phone, through e-mail or at the annual National Tasker Working Group conference.[5] As a result, change requests are not tracked in a consistent or documented manner. Therefore, documentation to support change requests is dispersed

[5] The purpose of the conference is to provide guidance from SJS and CJOC on tasking processes. It also allows organizations who supply military resources for taskings an opportunity to discuss current operations, manning concerns and other issues related to taskings. Some of these other related issues could include the alignment of CFTPO functionality to the tasking processes. The primary target audience are newly appointed taskers who manage taskings at the highest level of their organization, as well as the tasking community at large.

throughout various email communications between the MCSC and the user community, minutes of the annual National Tasker Working Group conference, and annotations in the application code.

Additionally, the approvals for all maintenance and major changes to the application were not formally documented. MCSC personnel noted that changes made to the CFTPO application are only documented as part of the application code. As a result, users and other stakeholders have limited visibility into the prioritization and tracking of changes made to the application. As previously mentioned, without documented business rules and requirements, the degree to which changes made to the CFTPO application faithfully meet these rules and requirements could not be verified.

According to MCSC personnel, any proposed CFTPO application changes beyond those considered minor would be reviewed before implementation by two senior analysts. MCSC personnel also indicated that changes would undergo testing and user acceptance in a testing environment before being implemented in the application. However, the audit team could not confirm whether this is taking place in an effective manner due to the lack of documentation.

Although most users interviewed were of the opinion that the changes they request are implemented, there was no evidence of a systematic and independent review of the application code to ensure its integrity. This results in a residual risk that the application may be performing, or allowing performance of, unintended functions. For example, there is a possibility that users who are not permitted to view the information of military members on operational taskings may be able to do so through one of the several interface views offered by the CFTPO application.

There are two contributing factors for this informal change management process. The first is the absence of formalized authorities, roles and responsibilities for change management. The second is the limited documentation that is commensurate with the software development method that the MCSC uses.

Throughout the development of the CFTPO application, the MCSC has subscribed to a software development approach that does not place as high a priority on the documentation of software changes as does the approach typically used in the DND/CAF. In contrast, this typical approach requires that each phase of development proceed in strict order, and that it be documented.

2.2.2 Conclusion

Without important system design documentation, continuity of the application is at risk as it is heavily dependent on the corporate memory of key MCSC personnel. As well, the availability of higher-level information about the system and changes would allow stakeholders to assess whether the application is performing functions as required by their business and by departmental policy.

ADM(RS) Recommendation

2. The CA should formalize the change management process for the CFTPO application to help ensure that changes to the application are authorized, documented and communicated, and that they function as intended and meet business needs.

OPI: CA

2.3 Application Controls

Although there are controls to address many of the technical aspects of data entry, processing, and output, the accuracy and completeness of data is deliberately and largely left up to users to assure.

Application controls are used to help ensure that the existing business rules are enforced and operate as intended. In the case of CFTPO, few business rules were documented, making it difficult to link existing application controls with these rules. For example, a tasking end date cannot be earlier than a tasking start date.

Additionally, two of the eight required fields documented in SJS standard operating procedures for incremental tasks requiring resources from other organizations were programmed as optional in the CFTPO application. Interviews with SJS personnel indicated that these standard operating procedures are internal documents, but if minimum requirements for taskings were not followed by other organizations they would not be accepted. Additionally, MCSC personnel noted that the enforcement of these fields was never explicitly requested by users or those responsible for the tasking process until the 2015 National Tasker Working Group annual meeting. A documented rationale as to why these business rules were not implemented was not found.

2.3.1 Input Controls

Input controls that ensure data is entered into the CFTPO application as intended exist for most input fields, although some fields allow for user flexibility. Data input fields were designated as mandatory or optional. The majority (85%) of the 210 personnel fields examined in the CFTPO application were controlled by being automatically populated, using a drop down list or selecting a date from an electronic calendar. The remaining fields (15%) can be typed in freely, with the only restriction being the type of characters that can be entered.

Good Practices

- There is a detailed transaction history that allows users to monitor and trace transactions.
- Built-in reporting capabilities accessible to users and management provide information on the degree of compliance with tasking requirements.

In some cases, key data held in other departmental information systems is not available to the CFTPO application. For example, the application does not have access to equipment data and financial codes from the Defence Resource Management Information System. This information is required to assign resources to taskings

with up-to-date equipment information and for potential expense allocation purposes. The need to manually input this data increases the risk of error.

2.3.2 Access Controls

CFTPO system access and authorization controls, as well as high-level descriptions of the permissions associated with the various types of user roles, are defined in the user manual. However, there is no approved definition by the respective stakeholders of what permissions the various roles should have or how they should be managed. Specific application role permissions and capabilities should reflect business rules. These rules have not been defined, which could increase the risk of inappropriate access to information.

Good Practices

- Once users log into the CFTPO application for the first time, their user identification is linked to their network identification, which ensures their exclusive access to the application.
- User privileges are restricted by those responsible for each particular task.
- Transactions performed by users in the application are logged.

Also, the process of granting and reviewing special access rights, such as how far back a user can make retroactive changes to data from the application, is informal. These rights, granted to users who may need to make retroactive corrections after a tasking, would normally be locked in the application. The process for granting and approving these rights is different in each user organization.

2.3.3 Processing Controls

Since the CFTPO application receives data from a number of external systems, controls are required to ensure that data integrity is maintained through the transfer of information. Processing controls are also needed to ensure that the system functions as expected, to detect errors and exceptions and to ensure the quality of data within the system.

Good Practices

- The process to upload data into CFTPO has controls in place to ensure that the root causes of upload errors are identified and addressed, and that the application is protected from the generation of new errors.

Weekly manual uploads of HRMS data result in outdated information in the CFTPO application database and are prone to human error. However, the CFTPO application provides on-screen reports that identify any reconciliation issues encountered during uploads.

There is no process established for taskers to conduct periodic data cleanups of incomplete and unused tasking activities, which may result in the reporting of incomplete or irrelevant information. Taskers perform correction activities on their input data as needed and monitor transactions on an ongoing basis. Also, MCSC staff have indicated that they perform weekly data quality monitoring through standard reports. This can include monitoring records to ensure a

tasker is not tasking themselves or ensuring that tasks follow intended processes in the CFTPO application.

2.3.4 Output Controls

The CFTPO application's reporting functionalities allow users to validate the accuracy and completeness of data in the CFTPO application. All users can access a built-in tool that has flexible reporting capabilities and that can generate reports on all taskings. These reporting capabilities give users the ability to verify transactions and to identify the source of reported errors. All reports can be exported into Excel spreadsheets. There are no documented restrictions as to who can export this data. Data exports are not tracked or monitored. Even though the CFTPO application's reporting and export functions are useful, there is a risk that users without proper training may make incorrect conclusions on generated reports, or that the data may be susceptible to inappropriate use.

2.3.5 Conclusion

The CFTPO application incorporates a variety of controls within key areas of the system to ensure the reliability of data. Input, access, processing and output controls are intended to protect the integrity of application data.

However, without a documented understanding of stakeholder requirements and work processes, the completeness and effectiveness of these controls could not be assessed. Improved documentation is needed in order to identify the workflows and requirements within the tasking process in order to translate them into business rules and application controls.

ADM(RS) Recommendation

3. The CA, in consultation with those responsible for the tasking process and the safeguarding of source data, should document and implement all key business rules related to data input, access, processing and output controls in the CFTPO application to help ensure that information is accurate and complete, and that it meets security and privacy considerations.

OPI: CA

2.4 Training

Not all taskers have been trained on how to use the CFTPO application, and the available instructional resources are neither current nor sufficiently detailed to meet all of their needs.

2.4.1 Management of Training Needs

Proper user training is required to optimize an application's use and value to the organization. There was no indication of a planned and concerted effort from the tasker community or the MCSC to ensure that users are provided with the necessary training.

Due to limited available training resources (i.e., one non-dedicated MCSC instructor) and the large number and geographical span of those requiring training, a train-the-trainer strategy is employed. In some cases, interviewees confirmed their past participation in training courses, while others indicated that most CFTPO application users do not benefit from formal training. Therefore, there is a risk that some users may not be able to correctly post transactions, run reports or interpret the information available to them.

Good Practices

- A basic application user manual and an online resource and training module are available to users.
- The MCSC provides formal training as requested and uses a training version of the CFTPO application to facilitate learning.
- Help desk support is available in case users require assistance with the application or need to report issues.

The application user manual, which also serves as the content for online training, has not been updated since 2010, and other available online resources offer very limited current and relevant information. The CFTPO application user manual has not been reviewed or approved by those responsible for tasking processes. In addition, none of the training material describes the full tasking workflow at a level of detail required by users to be able to adopt a self-study approach.

2.4.2 Conclusion

Improvements in the training material, together with relevant and timely training, would enhance users' understanding of the application and its role in the tasking process.

ADM(RS) Recommendation

4. The CA, in consultation with those responsible for the tasking process, should develop and implement a training program for the tasking process and for the CFTPO application, along with the appropriate supporting documentation.

OPI: CA

3.0 General Conclusion

Some of the necessary application controls have been implemented for the CFTPO application to help ensure the accuracy and completeness of the CFTPO application data. However, full implementation of application controls is complicated by the number of stakeholders responsible for the tasking process and the lack of documentation related to requirements. Business rules should be defined and agreed upon so as to ensure that the application meets the needs of those responsible for the tasking process and the safeguarding of source data. Based on agreed-upon business rules, appropriate action can be taken to ensure that only authorized changes are made to the application and that source data is protected and used as intended.

The recommendations were provided to strengthen the governance of the CFTPO application, to improve the documentation of the change management process and of the business rules that support application controls and to enhance related training in order to help ensure that tasking decisions are based on more accurate and complete information.

Annex A—Management Action Plan

ADM(RS) uses recommendation significance criteria as follows:

Very High—Controls are not in place. Important issues have been identified and will have a significant negative impact on operations.

High—Controls are inadequate. Important issues are identified that could negatively impact the achievement of program/operational objectives.

Moderate—Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations.

Low—Controls are in place but the level of compliance varies.

Very Low—Controls are in place with no level of variance.

Authorities and Responsibilities

ADM(RS) Recommendation (High Significance)

1. The CA, in consultation with those responsible for the tasking process and the safeguarding of source data, should define and implement the authorities and responsibilities for the development and management of the CFTPO application and for the acquisition of source data.

Management Action

(a) The CA (MCSC / Director Land Command and Information) has drafted a comprehensive Business Charter (BC) to define and formalize MCSC structures, processes, capabilities and a change management and governance process (including authorities and responsibilities) for MCSC applications. Under the DND/CAF Defence Application Strategy, approved at the Information Management Board in July 2016, the CA (Director Land Command and Information) is working with ADM(IM) / Director General Enterprise Application Services to strengthen the existing relationship, clarify and document principles and governance and establish a collaborative change management process. The first draft of the BC, which is to include the role of ADM(IM) and other partners in the Defence Application Strategy, is near completion with a target publication date of Fall 2016.

(b) On August 11, 2015, Commander Military Personnel Command exercised formal authority by issuing direction on authorized access to military personnel data from the corporate system of record. The MCSC has implemented the necessary data access controls and will remain responsive to implement future controls directed by Commander Military Personnel Command.

(c) The CA, in close collaboration with SJS, will determine if there is a DND/CAF requirement for DND civilian data to be accessible through the MCSC suite of applications, including CFTPO. If the requirement is confirmed, the CA will seek to obtain formal authority/direction from Assistant Deputy Minister (Human Resources – Civilian) to access

civilian personnel data, and will remain responsive to implement future application controls directed by Assistant Deputy Minister (Human Resources – Civilian). The CA will confirm with Director Human Resources Information Management if any other source data owners are implicated in the current CFTPO dataset and will seek necessary approvals for usage of data under their respective authorities.

(d) The CA will continue to collaborate with those responsible for source data to seek automated, timely (i.e., real-time) data feeds from systems of record in order to mitigate the risks to integrity, currency and validity of data within CFTPO and, by extension, within other MCSC applications.

(e) The CA will seek to identify functional authorities from across the CAF for each MCSC application to address the definition and implementation of any additional authorities and responsibilities deemed necessary for the development and management of MCSC applications. In the case of CFTPO specifically, it is understood that SJS, as the Level 0 tasker, will be the overarching functional authority and will collaborate with Level 1 taskers as required.

(f) ADM(IM) and functional authorities will become standing members of the MCSC Change Management Board, with specified responsibilities outlined in the BC. The CA held the inaugural MCSC Change Management Board in Spring 2016.

(g) Suggested Office of Collateral Interest (OCI): SJS.

OPI: CA
Target Date: May 2017

Change Management

ADM(RS) Recommendation (High Significance)

2. The CA should formalize the change management process for the CFTPO application to help ensure that changes to the application are authorized, documented and communicated, and that they function as intended and meet business needs.

Management Action

(a) As per the response in Authorities and Responsibilities, the MCSC BC and the stand-up of the Change Management Board will formalize the change management process for all MCSC applications, including CFTPO. Change Management Board Records of Decision will serve to document the business rules and authorizations for application changes.

(b) Service level agreements will be drafted annually, as required, between the CA and collaborating Level 1 organizations to formalize the list of functional change requests, identify appointed functional authorities and outline funding arrangements for each fiscal year. These service level agreements will become an important means of documenting new

business needs from the functional authorities, and will be reviewed at year-end to monitor progress and ensure changes reflect business needs.

(c) The CA will work collaboratively with SJS to formalize a CAF tasking governance framework, which will include a section on CFTPO change management that is aligned with the MCSC BC.

(d) Suggested OCI: SJS

OPI: CA
Target Date: May 2017

Application Controls

ADM(RS) Recommendation (Moderate Significance)

3. The CA, in consultation with those responsible for the tasking process and the safeguarding of source data, should document and implement all key business rules related to data input, access, processing and output controls in the CFTPO application to help ensure that information is accurate and complete, and that it meets security and privacy considerations.

Management Action

(a) MCSC has diligently applied DND/CAF policy and best practices in safeguarding data and will continue to use applicable processes, such as the Privacy Impact Assessment and the Security Assessment and Authorization Program. Existing reviews of security and privacy (Privacy Impact Assessment and Security Assessment and Authorization completed this fiscal year) were positive and provided valuable recommendations for improvement. Where a documented business need exists, Commander Military Personnel Command provides formal conditional authorization for MCSC to make military personnel data available to authorized MCSC users. The conditions include the requirement to appropriately encrypt data at rest and protect information in transit. Military personnel data in MCSC applications is managed at all times in accordance with approved Security Assessment and Authorization guidelines. These processes will continue to be used by the MCSC to reinforce best practices, ensure ongoing compliance and make continual incremental improvements as necessary.

(b) As per the response in Authorities and Responsabilities, the CA, in close collaboration with SJS, will seek to formalize a CAF tasking governance framework that will document key business rules related to data input, access, processing and output controls. The MCSC will play a supporting role, as required, in the definition of these business rules.

(c) The CA will ensure that the MCSC continues to document its software code, and will consider options to increase its resources in order to ensure the CFTPO help utility is updated when either new business rules are created, or extant rules are changed.

(d) MCSC applications depend on accuracy and, to a lesser degree, completeness of data. Collaborative efforts to ensure data accuracy and completeness, and to take corrective action

as needed, will be led or coordinated (as applicable) by the CA and will be reinforced through the BC and other engagement opportunities as noted throughout the management action plan.

(e) Suggested OCI: SJS

OPI: CA
Target Date: May 2017

Training

ADM(RS) Recommendation (Moderate Significance)

4. The CA, in consultation with those responsible for the tasking process, should develop and implement a training program for the tasking process and for the CFTPO application, along with the appropriate supporting documentation.

Management Action

(a) The CA will continue to provide a limited train-the-trainer capability for Level 1 OPIs of all MCSC applications, including CFTPO, in the near term based on the allocated resources. The CA will analyze the requirement to increase its train-the-trainer capacity and consider options to do so if necessary.

(b) The CFTPO "Help" button gives users access to four online links (CFTPO Wiki, CFTPO Discussion Board, Email to HelpDesk and CFTPO Web page). These links provide the training materials including the application user manual (Tasker Manual), a training package and other "help button" information. The Tasker Manual and other outdated material will be updated to match the current version of CFTPO and its functionality along with any commensurate changes to applicable business rules. The CA will strive to maintain currency on a best-effort basis within resources available (i.e., to minimize the lag between application changes and any resulting updates required to training materials) as changes to business rules and/or application functionality are implemented and ideally before the next round of training opportunities.

(c) Following formalization of the tasking framework by SJS, the CA will work collaboratively with them, as the functional authority for CFTPO, to ensure all stakeholders are updated on the tasking process during the annual National Tasking Working Group.

(d) Suggested OCI: SJS

OPI: CA
Target Date: May 2017

Annex B—Audit Criteria

Criteria Assessment

The audit criteria were assessed using the following levels:

Assessment Level and Description
Level 1: Satisfactory
Level 2: Needs Minor Improvement
Level 3: Needs Moderate Improvement
Level 4: Needs Significant Improvement
Level 5: Unsatisfactory

Objective

To provide assurance that appropriate application controls are in place to help ensure the accuracy and completeness of the CFTPO application data.

Criteria

1. All changes in software comply with a formal change management process.

   Assessment – Level 4. Application control changes could not be validated as the change management process is informal. Weaknesses related to practices for documenting and recording key information for changes need to be addressed.

2. Controls are in place to ensure that transactions are accurate and complete.

   Assessment – Level 3. Moderate improvement is required to define, document and approve all business rules, in conjunction with all relevant stakeholders, to ensure that transactions are accurate and complete and in line with stakeholder expectations. As well, weaknesses related to the documentation and accessibility of key application functions and controls need to be addressed.

3. Processes are in place to ensure that the integrity and validity of data is maintained throughout the processing cycle and the detection of erroneous transactions does not disrupt processing of valid transactions.

   Assessment – Level 2. Because of the reliance of CFTPO on external source data from other systems, many of the issues impacting the integrity and validity of data are outside the control of the CA. Collaboration with those responsible for the source data through formal agreements to receive timely data in an automated manner would reduce the risk of upload errors. As well, documenting data monitoring procedures for CFTPO application users would help reduce unneeded and erroneous data.

4. Controls are in place to ensure that output is designed, developed and generated as approved by those responsible for the tasking process.

   Assessment – Level 3. Moderate improvements could be made to gather and document user requirements in order to ensure that output is designed and developed in line with business needs.

5. Application system outputs are reviewed for reasonableness, accuracy and completeness, and potential errors are logged and addressed in a timely manner.

   Assessment – Level 2. Minor improvements could be made to ensure that the process for stakeholders to detect and communicate errors is documented and communicated.

Sources of Criteria

1. Institute of Internal Auditors. Global Technology Audit Guide 8: Auditing Application Controls, 2007.

2. ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012.

3. ISACA. COBIT 5 and Application Controls: A Management Guide, 2009.